Ośrodek Rozwoju Edukacji

Anna Turewicz-Lipczyńska

Ochrona danych osobowych

Poradnik dla dyrektora szkoły

Redaktor prowadzący
Katarzyna Koletyńska

Redakcja językowa i korekta
Katarzyna Gańko

Opracowanie graficzne i skład
Aneta Witecka

ISBN 978-83-62360-89-5

Ośrodek Rozwoju Edukacji
Aleje Ujazdowskie 28
00-479 Warszawa
tel. 22 345 37 00
fax 22 345 37 70

Spis treści

Podstawa prawna

Dyrektor placówki oświatowej powinien interesować się ochroną danych osobowych, ponieważ znajomość podstawowych przepisów prawnych normujących te zagadnienia oraz wprowadzenie w życie właściwych uregulowań pomogą uniknąć odpowiedzialności karnej, grzywny pieniężnej, a nawet kary ograniczenia lub pozbawienia wolności.

Funkcjonowanie szkół i innych placówek sektora oświaty nie jest możliwe bez wykorzystywania danych osobowych nauczycieli i innych pracowników szkoły, dzieci, ich rodziców oraz opiekunów prawnych; tym samym podlega rygorom określonym *Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* (tekst jednolity: Dz.U. 2014, poz. 1182), zwaną dalej „Ustawą".

Ustawa, rozwijając zagwarantowane w art. 51 Konstytucji RP prawo do ochrony danych osobowych, określa zasady postępowania przy ich przetwarzaniu oraz prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych. Ustawę stosuje się do przetwarzania danych osobowych w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych, jak również w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych.

Wojciech Rafał Wiewiórowski, Generalny Inspektor Ochrony Danych Osobowych, w rozmowie z Haliną Drachal z „Głosu Nauczycielskiego" stwierdził: „Dyrektorom szkół radziłbym dobrze zapoznać się z przepisami ustawy o ochronie danych osobowych, bo świetnie znają prawo oświatowe, ale ich wiedza na temat przetwarzania danych osobowych nie zawsze jest taka duża. A ustawa obowiązuje w każdej placówce oświatowej, zarówno w małej wiejskiej szkole, jak i placówce dużej, położonej w centrum metropolii – i to niezależnie od tego, czy jest ona prowadzona przez państwo, gminę czy stowarzyszenie" (Drachal, 2010, s. 9).

Realizacja zasad przetwarzania danych osobowych jest przede wszystkim obowiązkiem administratora danych, którym zgodnie z art. 7 pkt 4 Ustawy jest organ, jednostka

organizacyjna, podmiot lub osoba określająca cele i środki przetwarzania danych. Bardzo często o tym, kto jest administratorem danych, decydują przepisy szczególne.

Z taką sytuacją mamy do czynienia w przypadku szkoły. Oznacza to, że dyrektor w kierowanej przez siebie placówce ma zapewnić zgodne z prawem przetwarzanie danych osobowych, jak również ponosi odpowiedzialność za działania wszystkich osób upoważnionych do tego działania. Warto zauważyć, że obowiązki nałożone przez Ustawę na szkoły i kierujących nimi dyrektorów nie powinny być sprowadzane jedynie do wymogów o charakterze formalnym, których naruszenie może rodzić odpowiedzialność administracyjną, karną, dyscyplinarną czy cywilnoprawną. Trzeba widzieć je szerzej – jako element dobrego zarządzania placówką, w tym budowania odpowiednich relacji z rodzicami uczęszczających do niej uczniów.

Podstawowe pojęcia

Pojęcia, które występują w związku z wdrożeniem zapisów Ustawy:

Dane osobowe – w rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Tożsamość osoby możliwej do zidentyfikowania można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo specyficzne czynniki określające jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne (np. imię i nazwisko, adres, PESEL, NIP, wizerunek).

Zbiór danych – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony, czy podzielony funkcjonalnie (np. teczka, segregator, wydruk, skoroszyt, lista, dziennik itp.).

Przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych (takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie), zwłaszcza te, które wykonuje się w systemach informatycznych.

System informatyczny – zespół współpracujących ze sobą urządzeń, komputerów, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

Usuwanie danych – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby.

Administrator danych osobowych (ADO) – organ, jednostka organizacyjna, podmiot lub osoba decydujące o celach i środkach przetwarzania danych osobowych (zgodnie z Ustawą są to m.in. podmioty niepubliczne realizujące zadania publiczne, osoby fizyczne i osoby prawne oraz jednostki organizacyjne niebędące osobami prawnymi, jeżeli przetwarzają dane osobowe w związku z realizacją celów statutowych lub z działalnością zarobkową czy zawodową, a także organy państwowe, organy samorządu terytorialnego oraz państwowe i komunalne jednostki organizacyjne). **Administratorem danych osobowych jest ten, kto decyduje o celach i środkach przetwarzania danych, czyli szkoła, którą reprezentuje dyrektor.**

Zgoda osoby, której dotyczą dane – oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści, może być odwołana w każdym czasie.

Odbiorca danych – każdy, komu udostępnia się dane osobowe, z wyłączeniem osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, polskiego przedstawiciela podmiotu przetwarzającego dane, który ma siedzibę albo miejsce zamieszkania w państwie trzecim, podmiotu, któremu w drodze umowy powierzono przetwarzanie danych, oraz organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

Administrator bezpieczeństwa informacji (ABI) – dyrektor placówki lub wyznaczona przez niego osoba odpowiedzialna za zastosowane środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. W szczególności ABI powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Należy zauważyć, że dyrektor szkoły będzie wykonywał czynności ABI jedynie wtedy, gdy nie powierzy tych obowiązków innej osobie.

Lokalny administrator danych osobowych – pracownicy administracyjni szkoły, nauczyciele, pedagodzy specjalni, wychowawcy, bibliotekarze i inne osoby, które mają z tymi danymi do czynienia.

Administrator sieci – osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemów informatycznych służących do przetwarzania danych osobowych.

Osoba upoważniona (użytkownik) – osoba posiadająca upoważnienie wydane przez ADO – (dyrektora placówki lub osobę wyznaczoną).

Poufność danych — właściwość danych zapobiegająca ich nieuprawnionemu udostępnieniu nieupoważnionym podmiotom.

Identyfikator użytkownika (login) – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.

Hasło – ciąg znaków literowych, cyfrowych lub innych przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.

Uwierzytelnianie — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

Nośniki danych osobowych – płyty CD lub DVD, pamięć flash (pendrive'y), dyski twarde, taśmy magnetyczne lub inne urządzenia/materiały służące do przechowywania plików z danymi.

Obowiązkiem dyrektora każdej placówki jest staranna ochrona interesów osób, których dotyczą dane, a w szczególności zapewnienie, aby dane te były przetwarzane zgodnie z prawem, zbierane dla konkretnie oznaczonych, zgodnych z prawem celów, niepoddawane przetwarzaniu niezgodnemu z celami, dla których zostały zebrane.

Zebrane dane powinny być merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane (powinny być zbierane wyłącznie dane potrzebne do konkretnej

sprawy i tylko takie, które są dla danego celu niezbędne[1]). Dane należy przechowywać w postaci umożliwiającej identyfikację osób, których dotyczą. Dyrektor powinien w miarę posiadanych możliwości dążyć do unowocześniania stosowanych na terenie szkoły informatycznych, technicznych i organizacyjnych środków ochrony danych w celu zabezpieczenia danych osobowych przed udostępnianiem osobom nieupoważnionym, przetwarzaniem z naruszeniem przepisów o ochronie danych osobowych, nieautoryzowaną zmianą, uszkodzeniem lub zniszczeniem.

Gdzie znajdują się dane osobowe

W szkole znajdują się liczne zbiory danych osobowych. Przechowywane są one zarówno w sposób sformalizowany, jak i w formie rozproszonej. Podstawowe zasady dotyczące zapewnienia bezpieczeństwa w zakresie danych osobowych dotyczą danych przetwarzanych w:

- ✓ **zbiorach tradycyjnych**, w szczególności arkuszach ocen, orzeczeniach o potrzebie kształcenia specjalnego oraz wszelkich opiniach specjalistycznych (poradni psychologiczno-pedagogicznych, lekarskich), kartotekach, księgach uczniów, absolwentów, wypadków, rejestrach wydanych legitymacji, kart rowerowych i motorowerowych, dziennikach, teczkach wychowawców, dokumentach związanych z rekrutacją, skorowidzach, aktach osobowych, wykazach (np. wykazach osób korzystających z dofinansowania obiadów czy podręczników), podaniach o przyjęcie (do szkoły, świetlicy, na obiady itp.), w zbiorach ewidencyjnych, wszelkich zgodach (np. na uczestnictwo w zajęciach z religii, programach ogólnopolskich czy ogólnoszkolnych typu „Szklanka mleka", „Owoce w szkole" i innych);
- ✓ **dokumentacji związanej z przetwarzaniem danych wrażliwych**, w szczególności: dokumentacją dotyczącą programów dofinansowania do zakupu podręczników szkolnych (np. „Wyprawka"), programów socjalnych (np. stypendiów szkolnych, stypendiów specjalnych, pomocy finansowej, zapomóg, pożyczek wewnątrzzakładowych itp.);

[1] Ustawa nie zezwala na gromadzenie danych na wszelki wypadek lub też zbędnych dla danego procesu (np. w procesie rekrutacji).

- ✓ **listach motywacyjnych i podaniach o przyjęcie do pracy**, w tym osób niepracujących w danej szkole;
- ✓ **w systemach informatycznych**, w szczególności planach organizacyjnych, systemach ewidencji uczniów typu EdPlan, VULCAN i innych, systemach informatycznych prowadzonych przez jednostki nadzoru pedagogicznego (np. ewidencja związana z testami szóstoklasisty, egzaminami gimnazjalnymi, maturami, egzaminami zawodowymi itp.) oraz organy prowadzące (np. ewidencja w celu ustalania dotacji), w Systemie Informacji Oświatowej i innych, w zależności od lokalnych rozwiązań informatycznych;
- ✓ **w dokumentacji kadrowo-płacowej** – w deklaracjach ZUS, ewidencjach płacowych, informacjach skarbowych, ewidencjach statystycznych prowadzonych przez dyrektora, pracowników działu kadr oraz księgowych.

Praca nad wdrożeniem zapisów Ustawy w danej placówce powinna rozpocząć się od analizy, gdzie można natknąć się na dane osobowe. Następnie należy pogrupować dane według kategorii. Każda placówka może opracować własne wykazy zbiorów[2].

Nie można zapominać o tym, że szkoła za każdym razem, gdy wykorzystuje dane osobowe lub wizerunek ucznia/nauczyciela/rodzica w środkach masowego przekazu czy na stronach internetowych, powinna otrzymać na to stosowną zgodę. Zgoda może być udzielona jednorazowo na dany okres (np. na dany rok szkolny), ale powinna zawierać cel, w jakim się wykorzysta dane, oraz miejsce udostępnienia[3].

[2] Przykładowy wykaz zbiorów danych osobowych w szkole podstawowej – z opisem konkretnych segregatorów i teczek – znajduje się w załączniku nr 2.

[3] Przykładowa zgoda na publikację zdjęć na stronie internetowej znajduje się w załączniku nr 4.

Konieczna dokumentacja

Rodzaje dokumentacji pedagogicznej, sposób obchodzenia się z dokumentami oraz metody ich przechowywania i archiwizacji precyzują dokumenty odnoszące się do ochrony danych osobowych (np. art. 37 i 39 ust. 1 Ustawy, § 3 *Rozporządzenia 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. nr 100, poz. 1024). Przepisy dotyczące zasad i sposobu funkcjonowania placówek oświatowych z których podstawowe znaczenie mają *Ustawa z dnia 7 września 1991 r. o systemie oświaty* (tekst jednolity: Dz.U. 2004, nr 256, poz. 2572) i aktach do niej wykonawczych, np. rozporządzeniach dotyczących prowadzenia przez szkoły dokumentacji przebiegu nauczania działalności wychowawczej i opiekuńczej czy zasad udzielania i organizacji pomocy psychologiczno-pedagogicznej w publicznych przedszkolach, szkołach i placówkach.

W przypadku przedstawiania przez rodziców opinii, zaświadczeń czy orzeczeń z poradni psychologiczno-pedagogicznych, czyli tzw. danych wrażliwych, obowiązują bardziej restrykcyjne zasady postępowania wynikające zarówno z przepisów szczególnych (np. ww. rozporządzenia w sprawie zasad udzielania i organizacji pomocy psychologiczno-pedagogicznej w publicznych przedszkolach, szkołach i placówkach), jak i ustawy o ochronie danych osobowych.

Warto dokonać gruntownej analizy własnych dokumentów, aby zdefiniować „miejsca wrażliwe", czyli konkretne teczki, skoroszyty i segregatory, w których gromadzi się dane osobowe. Kolejnym działaniem powinno być opracowanie jednego spójnego dokumentu – zatytułowanego np. *Polityka (Instrukcja) bezpieczeństwa danych osobowych w Zespole Szkół nr 1 w Warszawie* – w którym wszelkie zbiory danych osobowych funkcjonujące w danej placówce zostaną zidentyfikowane, pogrupowane i opisane. W dokumencie tym należy również określić, kto i do czego będzie miał dostęp.

Co powinien zawierać taki dokument, aby był przydatnym narzędziem we wdrożeniu Ustawy? Poniżej znajduje się jego przykładowa zawartość.

Polityka bezpieczeństwa danych osobowych w placówce oświatowej/szkole – przykładowa zawartość

Rozdział 1. Postanowienia ogólne

Przykładowa zawartość:

- regulacje dotyczące ochrony danych osobowych w konkretnej placówce;
- rodzaje zbiorów (tradycyjne, informatyczne);
- definicje podstawowych pojęć;
- podstawy prawne;
- określenie obowiązków poszczególnych pracowników, a zwłaszcza dyrektora, w zakresie ochrony danych osobowych gromadzonych w placówce.

Rozdział 2. Wykaz zbiorów danych osobowych i systemów informatycznych lub modułów programowych używanych do ich przetwarzania

Przykładowa zawartość:

- wskazanie wszelkich miejsc, w których w danej placówce gromadzi się, przetwarza czy przechowuje dane osobowe[4].

Rozdział 3. Nadawanie uprawnień

Przykładowa zawartość:

- opis uprawnień (kto i do czego jest uprawniony), np. w systemie komputerowo-informatycznym;
- opis metod i środków uwierzytelnienia oraz procedur związanych z użytkowaniem ich i zarządzaniem nimi – rodzaje zabezpieczeń, loginy i hasła, harmonogram zmian, procedury rozpoczęcia, zawieszenia i zakończenia pracy;
- wszelkie informacje dotyczące tego, kto ma prawo gromadzić, przetwarzać i udostępniać dane;
- informacje dotyczące szkolenia pracowników w tym zakresie oraz zaznajamiania nowych pracowników z założeniami *Polityki bezpieczeństwa*.

Rozdział 4. Kopie zapasowe

Przykładowa zawartość:

[4] Przykładowy wykaz zbiorów w placówce oświatowej znajduje się w załączniku nr 2.

- opis procedur tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi do ich przetwarzania;
- informacje dotyczące sposobu, miejsca i okresu przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych.

Rozdział 5. Zabezpieczenie antywirusowe

Przykładowa zawartość:

- informacje dotyczące sposobu zabezpieczania systemu informatycznego przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego, oraz postępowania w sytuacjach szczególnych.

Rozdział 6. Udostępnianie danych

Przykładowa zawartość:

- wskazówki dotyczące udostępniania danych osobowych i sposobu odnotowania informacji o udostępnionych danych (komu można je udostępniać i na jakich zasadach, a także kto może je udostępniać).

Rozdział 7. Przechowywanie i konserwacja

Przykładowa zawartość:

- opis wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych;
- informacje dotyczące właściwych sposobów przechowywania danych tradycyjnych, czyli gromadzonych w wersji papierowej (dane powinny być przechowywane w odpowiednich, zamykanych szafkach; należy ustalić także zasady dostępu do kluczy, sposób opisywania segregatorów itp.).

Rozdział 8. Odpowiedzialność za naruszenia zapisów *Polityki bezpieczeństwa*

Przykładowa zawartość:

- ustalony przez dyrektora zakres odpowiedzialności za naruszenie zapisów Ustawy, a w konsekwencji ustaleń wewnętrznej polityki w tym zakresie, np. odpowiedzialność finansowa za instalację pirackiego oprogramowania, dyscyplinarna za ujawnienie danych osobom nieuprawnionym czy też konsekwencje służbowe.

Rozdział 9. Wzory upoważnień i zgód

Przykładowa zawartość:

- wzory upoważnień dla pracowników, wzory zgód związanych z obrotem danymi osobowymi i wizerunkiem i inne wypracowane w tym zakresie dokumenty wewnętrzne.

Uprawnienia

Nadawanie uprawnień

Dostęp do danych osobowych gromadzonych w zbiorach tradycyjnych może uzyskać wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych wydane przez dyrektora szkoły. Upoważnienie określa rodzaj zbioru, do którego pracownik ma dostęp, oraz wskazuje zbiory, które ma prawo tworzyć i które może przetwarzać. Zakres upoważnienia do przetwarzania danych powinien być ściśle powiązany z zakresem zadań, jakie określona osoba wykonuje u administratora danych. Warto również dodać, że zgodnie z art. 39 ust. 2 Ustawy osoby te obowiązane są zachowywać dane osobowe (oraz sposoby ich zabezpieczenia) w tajemnicy. Upoważnienia do przetwarzania danych osobowych przechowywane są w teczkach akt osobowych pracowników.

Kluczowymi osobami, które mają dostęp do niemal wszystkich danych osobowych – oprócz dyrekcji szkoły – są pracownicy sekretariatu/kancelarii szkoły oraz nauczyciele wychowawcy. To im należy poświęcić szczególną uwagę podczas nadawania uprawnień i przygotowywania do obsługi danych (tworzenia, przetwarzania i obrotu).

Szkolenie pracowników

Szczególnie ważne w kwestii zapewnienia przestrzegania przepisów o ochronie danych osobowych jest szkolenie pracowników. **Każdy pracownik szkoły powinien wiedzieć, czym są dane osobowe i w jaki sposób może naruszyć Ustawę, oraz znać wszelkie obowiązujące w danej placówce procedury w tym zakresie.**

Podczas wdrażania zapisów Ustawy warto przeprowadzić szkolenie wszystkich pracowników i zapoznać ich z zasadami obowiązującymi w placówce. Każdy nowo przyjęty pracownik powinien gruntownie zapoznać się z *Polityką bezpieczeństwa* i pisemnie potwierdzić znajomość tego dokumentu. Ułatwi to późniejsze ewentualne dochodzenie roszczeń z tytułu naruszenia zapisów Ustawy. Każdy nauczyciel powinien wiedzieć, do jakich danych (zbiorów) ma dostęp oraz w jakim zakresie może z nich korzystać. Musi być również świadomy, że ma prawny obowiązek zachowania danych osobowych w tajemnicy. **Szczegółowe uprawnienia przypisane do konkretnego zbioru warto ująć w *Polityce bezpieczeństwa* i pogrupować w zależności od stanowiska.**

Jako przykład niech posłuży nauczyciel wychowawca, który – aby poprawnie wykonywać swoją pracę – musi mieć dostęp do konkretnych zbiorów, takich jak dzienniki, orzeczenia, arkusze ocen itp. Niektóre z nich tworzy sam i je później przetwarza (np. dzienniki i przygotowywane na ich podstawie zestawienia semestralne, teczki wychowawcy), niektóre tworzy, ale nie przetwarza (np. arkusze ocen), do jeszcze innych ma tylko dostęp (np. orzeczenia). Pracownik sekretariatu/kancelarii zwykle ma dostęp m.in. do kart zapisu do szkoły (gromadzi je i przetwarza), do systemu ewidencji uczniów (tradycyjnego lub elektronicznego, np. VULCAN – tworzy i przetwarza ten zbiór, udostępnia dane). Są również pracownicy mający dostęp do danych szczególnie wrażliwych, np. pracownicy działu księgowości czy kadr, osoba zajmująca się obsługą stypendiów itp. Są też osoby, które w minimalnym stopniu mają dostęp do danych osobowych, ale dane te również są chronione, np. osoba zajmująca się wydawaniem obiadów finansowanych z pomocy społecznej. **Upoważnienie do gromadzenia i przetwarzania danych osobowych powinno mieć formę pisemną.**

Pracownik powinien wiedzieć, jakiego rodzaju dane ma prawo gromadzić, po co to robi (aby wyjaśnić te kwestie rodzicom uczniów) i w jakim celu zostaną one wykorzystane. Wszelkie działania prowadzące do sporządzenia jakichkolwiek zestawień, sprawozdań imiennych czy statystycznych (wykorzystujących zestawienia imienne, w tym SIO) to przetwarzanie danych osobowych. Należy jasno ustalić, zasady zapewnienia przestrzegania przepisów o ochronie danych osobowych. Każda z sytuacji powinna znaleźć odzwierciedlenie w upoważnieniu[5].

Nadawanie uprawnień do przetwarzania danych oraz rejestrowanie ich w systemie informatycznym

Obsługiwać system informatyczny służący do przetwarzania danych osobowych i zarządzać danymi gromadzonymi w zbiorach tradycyjnych może wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych wydane przez dyrektora szkoły. **Upoważnienia te są przechowywane w miejscu ustalonym przez dyrektora (np. w teczkach osobowych lub teczce z upoważnieniami).**

[5] Przykłady upoważnień znajdują się w załącznikach nr 4 i 5.

Dostęp do danych osobowych w systemach informatycznych

Dostęp do danych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu identyfikatora użytkownika i właściwego hasła lub podaniu właściwego hasła dostępu do stanowiska komputerowego.

Dyrektor lub upoważniona przez niego osoba, np. administrator systemu informatycznego, ustala niepowtarzalny identyfikator i hasło początkowe dla każdego użytkownika systemu informatycznego, który przetwarza dane osobowe. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego nie można przydzielić go innej osobie.

Większość systemów komputerowych rejestruje czynności zalogowanego użytkownika, co umożliwia łatwiejsze zidentyfikowanie go w sytuacji, gdy doszło do naruszenia zasad obrotu danymi osobowymi. Ponadto warto zainstalować bezpłatne oprogramowanie monitorujące wydruki drukarek[6].

Gdy dana osoba utraciła uprawnienia do dostępu do danych osobowych, należy niezwłocznie wyrejestrować jej identyfikator z systemu informatycznego, unieważnić hasło oraz podjąć inne stosowne działania w celu zapobieżenia dalszemu dostępowi tej osoby do danych. **Za realizację procedury rejestrowania i wyrejestrowywanie użytkowników w systemie informatycznym odpowiedzialny jest dyrektor szkoły lub wskazana przez niego osoba, np. ABI.**

[6] Przykład: ze szkolnego komputera wydrukowano listę uczniów z numerami PESEL, która następnie została wyrzucona do śmietnika (nie zniszczona w niszczarce, tylko zgnieciona). Znalazł ją rodzic, który szukał zagubionego trampka pierwszoklasisty. Mając przypisanych użytkowników do komputerów, łatwo ustalić, kto uruchamiał zadanie drukowania i jaki dokument drukował (z dokładnością do 1 minuty).

Metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

Dane osobowe są przetwarzane z użyciem dedykowanych serwerów i komputerów stacjonarnych. **Procedury pracy dotyczą komputerów, na których w jakikolwiek sposób przetwarzane są dane osobowe, np. komputerów:**

- **z systemami ewidencji uczniów, pracowników, programami księgowymi, kadrowo-płacowymi;**
- **na których drukowane są świadectwa i pozostawiane są bazy danych poszczególnych klas;**
- **na których nauczyciele przygotowują opinie o uczniach (np. do poradni), tworzą imienne zestawienia semestralne, wkładki do arkuszy ocen, listy uczniów, dane kontaktowe do rodziców itp.**

Procedury rozpoczęcia, zawieszenia i zakończenia pracy

Dane osobowe, których administratorem jest szkoła, mogą być przetwarzane sposobem tradycyjnym lub z użyciem systemu informatycznego tylko na potrzeby realizowania zadań statutowych i organizacyjnych szkoły.

Rozpoczęcie pracy użytkownika w dowolnym systemie informatycznym (np. Windows, Linux, Android, iOS itp.) następuje po poprawnym zalogowaniu się do systemu, czyli uwierzytelnieniu. Rozpoczęcie pracy w aplikacji (konkretnym programie) musi być przeprowadzone zgodnie z zasadami korzystania z danego programu, czasem program również wymaga logowania (np. VULCAN). Zakończenie pracy następuje po poprawnym wylogowaniu się z systemu oraz po uruchomieniu odpowiedniej dla danego systemu opcji jego zamknięcia zgodnie z instrukcją zawartą w dokumentacji (czyli zamknięciu systemu i wyłączeniu komputera). **Niedopuszczalne jest zakończenie pracy w systemie bez wykonania pełnej i poprawnej operacji wylogowania z aplikacji i poprawnego zamknięcia systemu.**

Monitory stanowisk komputerowych wykorzystywanych do przetwarzania danych osobowych, znajdujące się w pomieszczeniach, gdzie przebywają osoby nieposiadające upoważnień do przetwarzania danych osobowych, należy ustawić w taki sposób, aby uniemożliwić osobom postronnym wgląd w wyświetlane dane (szczególnie w sekretariacie, dziale kadr, księgowości, zwłaszcza na stanowiskach otwartych typu „recepcja"). Nie należy pozostawiać włączonego komputera bez nadzoru. Jeśli pracownik wychodzi z pomieszczenia, powinien pozostawić co najmniej włączony wygaszacz ekranu z hasłem. **Dyrektor ustala zasady nadzoru nas stanowiskiem w sytuacjach, gdy komputer pozostaje włączony, a pracownika przy nim nie ma.**

Wydruki i płyty CD/DVD oraz dyski przenośne

Wydruki oraz nośniki danych zawierające dane osobowe należy przechowywać w miejscu uniemożliwiającym ich odczytanie przez osoby postronne. W praktyce oznacza to, że płyty CD ze zdjęciami ze szkolnych imprez, kopie zapasowe systemów z danymi i zarchiwizowane dane z konkretnych stanowisk należy przechowywać w zamkniętej szafce.

Nieprzydatne wydruki oraz nośniki danych należy zniszczyć w stopniu uniemożliwiającym ich odczytanie, najlepiej w niszczarce dokumentów. W związku z tym warto zaopatrzyć się w niszczarkę płyt CD/DVD (obecnie w standardzie z wieloma niszczarkami papieru) lub ustalić obowiązek przecięcia płyty przed wyrzuceniem. Gdy szkoła nie ma możliwości zakupu niszczarki lub gdy chwilowo nie można z niej skorzystać, wyrzucone wydruki powinny być podarte/pocięte w stopniu uniemożliwiającym ich złożenie i odczytanie. Należy zwrócić szczególną uwagę na ponowne wykorzystywanie pojedynczo zadrukowanych stron (które z oszczędności mogą być wykorzystane jeszcze raz). Na odwrocie nie mogą znajdować się żadne dane osobowe ani zdjęcia. Podobne zasady dotyczą dysków przenośnych, w tym pendrive'ów. Należy wziąć przy tym pod uwagę zagrożenie wirusowe, ryzyko zgubienia małego przedmiotu, jakim jest np. pendrive, i dostanie się danych w niepowołane ręce oraz poziom zaufania do pracowników (zabezpieczenie stanowiska w domu prywatnym – dostęp współmałżonka, dzieci, innych członków rodziny, zabezpieczenie sieci wewnętrznej itp.).

Obecność innych osób

Ustalenia wymaga również przebywanie osób postronnych w pomieszczeniach, w których są przetwarzane dane. Jest to dopuszczalne tylko w obecności osoby upoważnionej. **W praktyce oznacza to, że nie można pozostawić rodzica samego w pokoju z dziennikiem czy przy włączonym komputerze itp.**

Pomieszczenia, w których przetwarzane są dane osobowe, należy zamykać na czas nieobecności osób zatrudnionych. Gdy użytkownik ma jakiekolwiek podejrzenia co do ingerencji w przetwarzane dane (np. ktoś coś skopiował, wydrukował, przegrał na pendrive'a, włamał się do komputera itp.), powinien niezwłocznie powiadomić o tym dyrektora szkoły.

Kopie zapasowe

Należy ustalić sposoby archiwizacji ubiegłorocznych danych (np. zdjęć) oraz tworzenia kopii zapasowych na wypadek awarii. Wśród informatyków krąży powiedzenie, że użytkownicy systemów dzielą się na dwie grupy: tych, którzy tworzą kopie zapasowe, oraz tych, którzy będą to robić. Kopia zapasowa to nagrane na nośniku wszelkie bazy danych i dane, które są przetwarzane w szkole.

Zbiory danych osobowych w systemie informatycznym można zabezpieczyć przed utratą lub uszkodzeniem, stosując łącznie wiele rozwiązań. Należą do nich:

- ✓ podłączenie do komputerów urządzeń zabezpieczających przed awarią zasilania lub zakłóceniami w sieci zasilającej (czyli podłączenie urządzeń do UPS-ów lub sieci z zabezpieczeniem przepięciowym);
- ✓ sporządzanie kopii zapasowych zgromadzonych danych;
- ✓ zainstalowanie programów chroniących dostęp do komputera osobom nieuprawnionym bez wiedzy użytkownika (programy typu Internet Security, antywirusy);
- ✓ nieustanne szkolenie/doszkalanie pracowników.

Pełne kopie zapasowe zbiorów danych powinny być tworzone co najmniej dwa razy w ciągu roku, po zakończeniu typowego semestru. W przypadku danych księgowo-

płacowych, systemów ewidencyjnych itp. można ustalić inną częstotliwość tworzenia kopii (np. co miesiąc). W szczególnych sytuacjach, np. przed aktualizacją lub zmianą oprogramowania czy systemu, należy bezwzględnie wykonać pełną kopię zapasową.

Kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia w przypadku awarii systemu. Za przeprowadzenie tych czynności odpowiadają użytkownicy systemów informatycznych. Nośniki danych po ustaniu ich użyteczności należy wyczyścić z danych lub zniszczyć w sposób uniemożliwiający ich odczytanie.

Okresowe kopie zapasowe wykonywane są na płytach CD/DVD lub innych elektronicznych nośnikach informacji. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie – np. w szafie pancernej. **Dyrektor powinien ustalić okres przechowywania poszczególnych rodzajów kopii** (np. kopie semestralne przechowuje się przez rok). Kopie zapasowe należy bezzwłocznie usuwać po ustaniu ich użyteczności. **Za zniszczenie poszczególnych kopii zapasowych, jak również za dbałość o ich przydatność i aktualność, odpowiedzialny jest ten, kto został upoważniony/zobowiązany do ich wykonania.** Przez zniszczenie nośników informacji rozumie się ich trwałe i nieodwracalne zniszczenie fizyczne (np. płyty – zniszczenie w niszczarce do płyt lub pocięcie nożycami, w przypadku innych nośników zapisu informacji, typu dysk przenośny czy pendrive – co najmniej usunięcie danych i sformatowanie dysku)[7].

Hasła

Aby zapewnić minimum bezpieczeństwa podczas korzystania z komputerów, programów i systemów, **należy ustalić pewien kanon nadawania haseł, częstotliwość ich zmiany, przechowywania haseł oraz udostępniania ich osobom trzecim**.

Zgodnie z dobrą praktyką informatyczną dobre hasło użytkownika powinno mieć minimum 8 znaków, oprócz małych i wielkich liter powinno zawierać ciąg znaków alfanumerycznych i specjalnych, nie może zawierać żadnych informacji, które łatwo skojarzyć z użytkownikiem

[7] „Co najmniej" oznacza, że w sytuacji danych szczególnie wrażliwych, np. kadrowo-płacowych, księgowych, ewidencji uczniów, należy dołożyć dodatkowej staranności, aby dane np. z wyrzucanego dysku nie mogły zostać odtworzone za pomocą specjalistycznych programów do odzyskiwania danych.

komputera, np. jego danych osobistych, tj. nazwiska, inicjałów, imienia, marki lub numeru rejestracyjnego samochodu, imion dzieci itp. Hasło wpisywane z klawiatury powinno pojawiać się na ekranie jako ciąg jednakowych znaków (np. gwiazdek, kropek), nie powinno wyświetlać się w formie jawnej.

Hasło nie powinno być zapisywane w miejscu dostępnym dla osób nieuprawnionych. Użytkownik nie może udostępnić swojego loginu (identyfikatora), hasła oraz dostępu do stanowiska roboczego po uwierzytelnieniu w systemie osobom nieuprawnionym ani żadnej osobie postronnej. Hasło należy utrzymywać w tajemnicy, również po upływie jego ważności, a raz użyty login nie może być wykorzystany ponownie dla innego pracownika (nawet gdy poprzedni nie jest już zatrudniony). **Miejsce zdeponowania haseł powinien ustalić dyrektor placówki**. Może to być **rejestr haseł** przechowywany np. w szafie pancernej. Nie należy deponować haseł dla użytkowników systemów lokalnych, które w przypadku zapomnienia może zresetować administrator systemu lub sam użytkownik. W systemach lokalnych deponowaniu powinny podlegać tylko hasła użytkowników z uprawnieniami administracyjnymi dla danego systemu.

Należy pamiętać, aby podczas naprawiania sprzętu komputerowego przez osoby/firmy z zewnątrz nadzorować pracę z komputerem, w którym są przechowywane szczególnie wrażliwe dane (np. baza danych uczniów, orzeczenia o niepełnosprawności itp.). Nie należy też pochopnie podawać hasła takim osobom. Jeśli jest to konieczne, natychmiast po zakończeniu pracy należy zmienić podane hasło na inne. Natychmiastowa zmiana hasła zalecana jest również w sytuacji, gdy mogła je poznać osoba nieuprawniona (np. przez przypadek lub gdy istnieje nawet niewielkie prawdopodobieństwo, że hasło nie było właściwie chronione).

Zwykle systemy informatyczne, z których korzysta szkoła, wymuszają określoną częstotliwość zmiany hasła (np. systemy SIO, HERMES, EdPlan – co 30 dni; OPERON, Sprawdzian Kompetencji Trzecioklasisty – ustala administrator systemu OPERON; Centralna Komisja Egzaminacyjna, Ogólnopolskie Badanie Umiejętności Trzecioklasistów – ustala administrator systemu CKE). Podobne ustalenia należy przyjąć co do haseł nadawanych lokalnie.

Bezpieczeństwo a czynnik ludzki

Zabezpieczenie antywirusowe

Komputery wykorzystywane do przetwarzania danych osobowych powinny być szczególnie zabezpieczone przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego (programy typu *malware*[8], np. trojany[9], *backdoory*[10], wirusy[11], *spyware*[12] itp.). Na rynku dostępne są programy antywirusowe oraz bardziej rozbudowane programy typu Internet Security, oferujące dodatkowo np. ochronę poczty, *firewall* i inne usługi zabezpieczające. Na potrzeby tego poradnika wszelkie tego rodzaju oprogramowanie chroniące określa się mianem **antywirusów**.

Szczególnie starannie należy chronić komputery podłączone do sieci (zarówno wewnętrznej, jak i internetowej). Wirusy komputerowe oraz inne programy szpiegujące, włamujące się, działające w tle, wykradające dane itp. mogą pojawić się w systemach szkoły za pośrednictwem internetu, nośników informacji – płyt CD, dysków przenośnych, pendrive'ów – a także pobranych z internetu programów oraz linków i załączników przysyłanych pocztą elektroniczną itp. Aby zminimalizować straty związane nie tylko z nieuprawnionym dostępem

[8] *Malware* (ang.) to złośliwe oprogramowanie, wszelkie programy działające na szkodę użytkownika.

[9] Trojan (koń trojański) to program, który podszywa się pod ciekawe lub przydatne dla użytkownika aplikacje, gdy tymczasem dodatkowo instaluje różne ukryte, niepożądane funkcje (np. programy szpiegujące, bomby logiczne, furtki umożliwiające przejęcie kontroli nad systemem przez nieuprawnione osoby itp.), często działa w sposób niewidoczny dla użytkownika.

[10] *Backdoor* (ang.) to umyślnie utworzona luka w zabezpieczeniach systemu, która zostanie wykorzystana w przyszłości. *Backdoor*, czyli tzw. tylne drzwi, może być pozostawiony np. przez *crackera*, który włamał się przez inną lukę w oprogramowaniu (jej przydatność jest ograniczona czasowo do momentu usunięcia – np. program testowy na 15 dni, wersja demo programu itp). Często *backdoor* dostaje się do systemu poprzez konia trojańskiego.

[11] Wirus to program, który po zainfekowaniu komputera może działać na jego szkodę. Typowe działania wirusów: nieupoważnione kasowanie danych, rozsyłanie spamu pocztą elektroniczną, kradzież danych (hasła, numery kart płatniczych, dane osobowe), zatrzymanie pracy komputera, w tym całkowite wyłączenie, utrudnienie lub uniemożliwienie pracy użytkownikowi komputera (komputer pracuje coraz wolniej, niektóre aplikacje się nie uruchamiają), aż do działań uszkadzających np. dysk.

[12] *Spyware* (ang.) to programy szpiegujące, które zbierają informacje o użytkowniku bez jego zgody, np. informacje o odwiedzanych stronach internetowych, hasła dostępowe (np. do poczty, banków itp.). Występują często jako dodatkowy i ukryty komponent większego programu (np. nielegalnej kopii oprogramowania czy tzw. wersji scrackowanej itp.), odporny na usuwanie i ingerencję użytkownika.

do danych, lecz także z uszkodzeniem systemu czy sprzętu, należy wyposażyć komputery w oprogramowanie skanujące.

Skanowanie i szkolenie

Warto ostrzec w tym miejscu przed łatwo dostępnymi w internecie darmowymi programami, które bardzo często nie zapewniają skutecznej i aktualnej ochrony, a czasami zamiast skanować dane, kopiują je do sieci. Zainstalowany program antywirusowy powinien być tak skonfigurowany, by co najmniej raz w tygodniu (a najlepiej codziennie) dokonywał aktualizacji bazy wirusów oraz skanował nowe pliki, zaś co najmniej raz w miesiącu wykonywał pełne skanowanie systemu. Elektroniczne nośniki informacji, takie jak dyski przenośne, należy każdorazowo sprawdzać programem antywirusowym przed użyciem, po zainstalowaniu ich w systemie. Powyższą czynność realizuje użytkownik systemu. Zwykle trwa to tylko chwilę, wystarczy jedno kliknięcie myszką. W przypadku problemów ze sprawdzeniem zewnętrznego nośnika danych użytkownik jest zobowiązany zwrócić się z tym do administratora bezpieczeństwa informacji.

Komputery i systemy pracujące muszą mieć zainstalowany program antywirusowy, a w przypadku komputerów z dostępem do internetu – posiadać także oprogramowanie i mechanizmy zabezpieczające przed nieautoryzowanym dostępem z sieci (*firewall*). W przypadku gdy użytkownik stanowiska komputerowego zauważy komunikat oprogramowania zabezpieczającego system, który wskazuje na zaistnienie zagrożenia lub sam rozpozna tego typu zagrożenie, zobowiązany jest zaprzestać jakichkolwiek czynności w systemie i niezwłocznie skontaktować się z administratorem szkolnej pracowni komputerowej lub dyrektorem szkoły.

Warto w tym miejscu zauważyć, jak ważne jest szkolenie pracowników. Zwykle tego rodzaju komunikaty zawierają konkretną informację – wystarczy ją przeczytać i podjąć decyzję, co należy robić. Najczęściej program proponuje usunięcie pliku, wyleczenie go lub zignorowanie komunikatu. Należy wyczulić użytkowników, którzy nie mają szerokiej wiedzy informatycznej, aby uważnie czytali komunikat. Trzeba pamiętać, że niewłaściwa decyzja może zaszkodzić całej placówce.

E-mail

Na uwagę zasługuje również korzystanie z poczty elektronicznej (e-mail). Z badań[13] wynika, że infekcje systemów powstają najczęściej z winy użytkowników (Securelist, b.r.). Przy korzystaniu z poczty elektronicznej należy zwrócić szczególną uwagę na otrzymywane załączniki dołączane do treści wiadomości. **Pracownicy powinni wiedzieć, czy wolno otwierać własną pocztę na komputerach szkolnych, a jeśli tak, to jakie należy podjąć kroki, aby zminimalizować ryzyko infekcji. Użytkownicy powinni mieć jasność co do tego, że ich działanie może wpłynąć na pracę całej placówki.** Nierozsądny byłby zakaz korzystania z prywatnej poczty, warto jednak ustalić, że zabrania się np. otwierania załączników i wiadomości od niezaufanych nadawców. Ponadto w szkołach często jest sieć Wi-Fi, z której mogą korzystać nauczyciele. Warto prowadzić rejestr osób upoważnionych do korzystania w ten sposób z sieci oraz przeszkolić pracowników o związanych z tym zagrożeniach.

Nieuprawnione instalacje

Użytkownicy komputerów powinni wiedzieć, że nie mogą wyłączać, blokować czy odinstalowywać programów zabezpieczających komputer. Często zdarza się, że źle dobrany antywirus spowalnia system, a skanowanie bywa denerwujące i czasem jest zatrzymywane lub wyłączane.

Należy uświadomić użytkownikom, jakie ryzyko wiąże się z samodzielną instalacją oprogramowania, w szczególności nielicencjonowanego, na wszystkich komputerach. Należy również ustalić zakres odpowiedzialności cywilnej i finansowej za niezastosowanie się do tych zapisów (włącznie z kosztami ponownej instalacji systemu czy karą, która może być nałożona przez sąd za korzystanie z programu bez wymaganej licencji). Nie oznacza to, że najbezpieczniej będzie całkowicie zabronić korzystania z komputerów szkolnych. Trzeba przede wszystkim zwiększać świadomość pracowników oraz wypracowywać odpowiedzialność za podejmowane działania.

[13] Badania nad ryzykiem korzystania ze Skype'a, według których w 44% przypadków zagrożenie stanowił nie program, a korzystający z niego człowiek.

Osoby korzystające z komputerów (oraz systemów Obieg, VULCAN, EdPlan itp.), na których przetwarzane są dane osobowe, muszą przestrzegać kilku podstawowych zasad. Zabronione powinny być m.in.:

- ✓ ujawnianie loginu i hasła współpracownikom i osobom z zewnątrz;
- ✓ pozostawianie haseł w miejscach widocznych dla innych osób;
- ✓ udostępnianie osobom nieuprawnionym stanowisk pracy wraz z danymi osobowymi;
- ✓ udostępnianie osobom nieuprawnionym programów i systemów komputerowych, z których korzysta placówka (licencja jest najczęściej przypisana do placówki; w sytuacji niejednoznacznej odpowiedzialność ponosi właściciel licencji);
- ✓ używanie oprogramowania w innym zakresie niż pozwala na to umowa licencyjna;
- ✓ przenoszenie programów komputerowych (z licencją jednostanowiskową) lub dysków twardych z jednego stanowiska na inne;
- ✓ kopiowanie danych na nośniki informacji (płyty CD/DVD, pendrive'y), kopiowanie na inne systemy (np. do obszaru Cloud lub innych dysków w tzw. chmurze) w celu wyniesienia ich poza szkołę;
- ✓ samowolne instalowanie i używanie jakichkolwiek programów komputerowych, w tym również programów do użytku prywatnego;
- ✓ używanie nośników danych udostępnionych przez osoby postronne;
- ✓ otwieranie załączników i wiadomości poczty elektronicznej od nieznanych i niezaufanych nadawców;
- ✓ używanie nośników danych niesprawdzonych, niewiadomego pochodzenia lub niezwiązanych z wykonywaną pracą (jeśli użycie takich nośników jest konieczne, należy przeskanować je programem antywirusowym);
- ✓ tworzenie kopii zapasowych niechronionych hasłem i/lub bez odpowiednich zabezpieczeń miejsca ich przechowywania.

Postępowanie z przedmiotami zawierającymi dane osobowe lub umożliwiającymi dostęp do nich

Przedmioty zawierające dane osobowe to dokumenty i ich kopie, wydruki, zestawienia, ręczne notatki, podpisy na listach, listy obecności (np. rodziców na zebraniu), płyty CD/DVD, pendrive'y i inne nośniki, np. karty pamięci z telefonów i aparatów fotograficznych. Wyrzucenie takich przedmiotów bez uprzedniego trwałego zniszczenia i pozostawienie dokumentów w kopiarkach czy drukarkach niesie za sobą poważne zagrożenie, że dostaną się

one w ręce osób postronnych. Zagrożeniem będzie również pozostawianie kluczy w drzwiach, szafach, biurkach czy zostawianie otwartych pomieszczeń, w których przetwarza się dane osobowe. Komputery nie powinny pozostawać włączone i niezabezpieczone, należy zabezpieczyć hasłem chociażby wygaszacz monitora. Ponadto należy zwracać uwagę na otwarte szafki, w których znajdują się dane osobowe – powinny one być zamknięte na klucz, który zawsze musi być wyjęty z zamka. Nie powinno się zostawiać bez nadzoru osób trzecich przebywających w pomieszczeniach szkoły, nie należy też ignorować nieznanych osób z zewnątrz poruszających się w obszarze przetwarzania danych osobowych. Należy wyczulić pracowników na pozostawianie dokumentów na biurku po zakończonej pracy czy też pozostawianie otwartych dokumentów na ekranie monitora oraz uświadomić im (także pracownikom obsługowym – woźnym, stróżom itp.), jak ważne jest nieprzekazywanie informacji będących danymi osobowymi osobom nieupoważnionym. Każdy pracownik powinien więc znać obowiązujące ustalenia w tym zakresie.

Należy pamiętać, że do ochrony przedmiotów i komputerów zawierających dane osobowe przyczynią się:

- ✓ posługiwanie się własnym loginem i hasłem w celu uzyskania dostępu do systemów informatycznych;
- ✓ tworzenia haseł trudnych do odgadnięcia dla innych;
- ✓ nieprzerywanie procesu skanowania przez program antywirusowy na komputerze;
- ✓ wykonywanie kopii zapasowych danych przetwarzanych na stanowisku komputerowym, zabezpieczenie sprzętu komputerowego przed kradzieżą lub nieuprawnionym dostępem do danych;
- ✓ stałe szkolenie pracowników w tym zakresie i uwrażliwianie na kwestie ochrony danych osobowych.

Zalecenia w zakresie przetwarzania danych osobowych sposobem tradycyjnym

Miejscami tworzenia, uzupełniania i przechowywania dokumentacji dotyczącej przetwarzania danych osobowych sposobem tradycyjnym są pomieszczenia w placówce: sekretariat, pokój nauczycielski, gabinet dyrektora, gabinet rewalidacyjny, biblioteka, świetlica, klasy lekcyjne, pracownia komputerowa. **Osoby prowadzące dokumentację zobowiązane są do zachowania tajemnicy służbowej. Dokumentacji zawierającej dane osobowe nie można wynosić poza teren szkoły (również w formie elektronicznej).** Szczególną uwagę należy

zwrócić na wynoszenie dokumentów w celu uzupełnienia ich w domu przez nauczyciela, np. arkuszy ocen, dzienników lekcyjnych itp. Takie praktyki powinny zostać stanowczo zakazane. Niezależnie od poziomu zaufania do pracownika i jego doświadczenia zawodowego wystarczy uruchomić wyobraźnię, aby dostrzec jak potężne jest to zagrożenie dla obrotu danymi (członkowie rodziny, goście, dzieci, telefony z kamerkami, aparatami fotograficznymi, ryzyko zagubienia, kradzieży itp.).

Nieaktualna dokumentacja zawierająca dane osobowe powinna być archiwizowana lub niszczona zgodnie z ustaleniami obowiązującymi w placówce. Osoby prowadzące dokumentację zobowiązane są do niezwłocznego poinformowania dyrektora placówki o podejrzeniu, że osoby nieupoważnione mogły mieć dostęp do dokumentacji.

Przetwarzanie danych osobowych przez sekretariat/kancelarię powinien być odnotowany – z podaniem rodzaju przetworzonych/przekazanych danych, wskazaniem osoby, której przekazano dane, lub instytucji, do której skierowano informację zawierającą dane osobowe, oraz daty wykonania czynności. Na dokumencie powinny znaleźć się także nazwisko i podpis osoby dokonującej czynności. Warto założyć rejestr obrotu danymi.

Często spotykaną praktyką jest udostępnianie dziennika podczas zebrania z rodzicami lub wysyłanie uczniów po dziennik. Warto pamiętać, że dziennik zawiera większość danych osobowych ucznia, łącznie z numerami PESEL. Zabronione jest udostępnianie dzienników lekcyjnych osobom nieupoważnionym do przetwarzania zawartych w nich danych, w szczególności uczniom. Natomiast rodzice mają prawo wglądu w stopnie wystawiane swoim dzieciom w dzienniku, ale wyłącznie w taki sposób, aby nie mogli zobaczyć ocen innych uczniów. Jeśli w placówce panuje praktyka udostępniania sprawdzianów z tzw. teczki sprawdzianów, należy udostępniać je wyłącznie indywidualnie; rodzice nie powinni samodzielnie szukać sprawdzianu swojego dziecka.

W przeszłości, zwłaszcza podczas zebrań z rodzicami, praktykowano informowanie o poszczególnych uczniach. **Aby nie naruszać zapisów ustawy, informacji o uczniach, ich ocenach, postępach, zachowaniu, rodzaju zajęć, w których uczestniczą, można udzielać wyłącznie rodzicom lub osobom upoważnionym przez nich pisemnie.** Jeśli rodzic wyraził

zgodę na publikację informacji o sukcesach dziecka, podczas spotkania można wymienić np. stypendystów, laureatów nagród itp., warto jednak ustalić ten fakt wcześniej z rodzicem.

Ochronie podlega również uczestnictwo dziecka w zajęciach z religii i wychowania do życia w rodzinie lub innych zajęciach. **Stąd deklaracja zgody/braku zgody nie może mieć charakteru listy, powinna być wypełniana indywidualnie.**

Prawa i obowiązki osób chroniących dane oraz osób, których te dane dotyczą

Prawa osób, których dane są gromadzone

Przetwarzanie danych osobowych jest regulowane Ustawą. Zgodnie z art. 32 Ustawy każdej osobie przysługuje prawo do kontroli przetwarzania danych, które jej dotyczą, zawartych w zbiorach danych. Każdy ma prawo do ochrony dotyczących go danych osobowych, a zwłaszcza prawo do:

- ✓ uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy, a w przypadku gdy administratorem danych jest osoba fizyczna – jej miejsca zamieszkania oraz imienia i nazwiska;
- ✓ uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze;
- ✓ uzyskania informacji, od kiedy przetwarza się w zbiorze dotyczące go dane, oraz podania w powszechnie zrozumiałej formie treści tych danych;
- ✓ uzyskania informacji o źródle, z którego pochodzą dotyczące go dane, chyba że administrator danych jest zobowiązany do zachowania w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej;
- ✓ uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane;
- ✓ żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem Ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane;
- ✓ w określonych przypadkach – wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na szczególną sytuację;
- ✓ w określonych przypadkach – cofnięcia zgody na przetwarzanie danych osobowych, gdy administrator zamierza je przetwarzać w celach marketingowych, lub przekazywanie ich innemu administratorowi danych.

Obowiązek informacyjny administratorów danych

W przypadku zbierania danych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować ją o adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem jest osoba fizyczna – o miejscu swojego zamieszkania oraz imieniu i nazwisku. Ponadto administrator zbierający dane musi wskazać cel zbierania danych, a w szczególności poinformować o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach czy kategoriach odbiorców danych, poinformować o prawie dostępu do treści swoich danych oraz do ich poprawiania, a także o dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje – o jego podstawie prawnej. Dobrym rozwiązaniem jest wypracowanie takiej informacji i dołączenie jej np. do karty zapisu ucznia do szkoły lub innego dokumentu wypełnianego podczas przyjmowania ucznia. Przykładowa informacja dla rodzica dołączona jest do tej publikacji i może stanowić punkt wyjścia do opracowania własnej informacji[14]. **Przy podaniu o przyjęcie do szkoły warto również zamieścić zgodę rodzica na przetwarzanie danych osobowych dziecka, ponieważ w chwili złożenia podania nie jest ono jeszcze uczniem szkoły, a jego dane będą przetwarzane w procesie rekrutacji.**

Kontrola

Realizacją zapisów Ustawy zajmuje się w Polsce Generalny Inspektor Ochrony Danych Osobowych. Ma on uprawnienia do kontroli podmiotów zajmujących się danymi osobowymi, podejmowania działań zmierzających do zwiększenia zakresu ochrony tych danych oraz nakazania wszczęcia postępowania dyscyplinarnego, a także wydania odpowiedniej decyzji administracyjnej.

Jeżeli na podstawie wyników kontroli zostanie stwierdzone naruszenie zapisów Ustawy, inspektor może żądać wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom winnym dopuszczenia do uchybień. W przypadku naruszenia przepisów o ochronie danych osobowych Generalny Inspektor z urzędu lub na wniosek osoby zainteresowanej, w drodze decyzji administracyjnej, nakazuje przywrócenie stanu zgodnego z prawem, a w szczególności:

- ✓ usunięcie uchybień;
- ✓ uzupełnienie, uaktualnienie, udostępnienie lub nieudostępnienie danych osobowych;

[14] Np. podpis rodzica pod podaniem, a następnie notka informacyjna i podpis pod notką.

- ✓ zastosowanie dodatkowych środków zabezpieczających zgromadzone dane osobowe;
- ✓ wstrzymanie przekazywania danych osobowych do państwa trzeciego;
- ✓ zabezpieczenie danych lub przekazanie ich innym podmiotom;
- ✓ usunięcie danych osobowych.

W przypadku gdy przepisy innych ustaw regulują odrębnie wykonywanie czynności związanych z gromadzeniem czy przetwarzaniem danych osobowych, stosuje się przepisy tych ustaw.

Konsekwencje prawne naruszenia zapisów Ustawy

W przypadku niezastosowania się do decyzji Generalnego Inspektora Danych Osobowych na podmiot, do którego została skierowana decyzja, może zostać nałożona grzywna w celu przymuszenia. Zgodnie z treścią art. 119 *Ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji* (Dz.U. 2012 nr 1015, z późn. zm.) grzywnę w celu przymuszenia nakłada się, gdy egzekucja dotyczy spełnienia obowiązku znoszenia lub zaniechania albo obowiązku wykonania czynności – szczególnie takiej, której za zobowiązanego nie może wykonać inna osoba. Grzywnę nakłada się również, jeżeli zastosowanie innego środka egzekucji obowiązków o charakterze niepieniężnym nie jest celowe. Taka grzywna może być nakładana kilkakrotnie (zarówno na osoby fizyczne, jak i osoby prawne, a także na jednostki organizacyjne nieposiadające osobowości prawnej) w tej samej lub wyższej kwocie.

Zgodnie z treścią art. 49 Ustawy ten, kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne lub nie jest do tego uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch. Jeżeli to działanie dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne[15] lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia[16], kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech. Wymiar grzywny określa art. 33 Kodeksu karnego. Natomiast art. 34 mówi, że jeżeli Ustawa nie stanowi inaczej, kara ograniczenia wolności trwa od 1 do 12 miesięcy.

[15] Na przykład informacja dotycząca lekcji religii w szkole.
[16] Na przykład informacje zawarte w orzeczeniu o potrzebie kształcenia specjalnego.

Zgodnie art. 51 Ustawy ten, 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 dwóch. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku. Jeżeli administrator danych osobowych, administrując danymi, narusza – choćby nieumyślnie – obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, stosownie do treści art. 52 Ustawy podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Jeżeli podmiot przetwarzający dane osobowe tworzy zbiory danych, których pomimo obowiązku nie zgłasza do rejestracji zbioru danych, zgodnie z treścią art. 53 Ustawy podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku (Roszak, 2013).

Administrator ma obowiązek poinformowania osoby, której dotyczą dane, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w Ustawie. Kto nie dopełnia tego obowiązku, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku (art. 54).

Zgodnie z art. 19 Ustawy w razie stwierdzenia, że działanie lub zaniechanie kierownika jednostki organizacyjnej, jej pracownika lub innej osoby fizycznej będącej administratorem danych wyczerpuje znamiona przestępstwa określonego w Ustawie, Generalny Inspektor kieruje do organu powołanego do ścigania przestępstw zawiadomienie o popełnieniu przestępstwa, dołączając dowody dokumentujące podejrzenie.

Udostępnianie i powierzanie danych

Prawo do wglądu w dane osobowe ma osoba, której one dotyczą, a w przypadku osoby nieletniej – rodzic/opiekun prawny lub inna osoba upoważniona przez rodzica/opiekuna prawnego.

Prawo do gromadzenia i przetwarzania posiadają również osoby pisemnie upoważnione przez dyrektora placówki w zakresie niezbędnym do wykonywania swoich obowiązków (np. wychowawca, pedagog specjalny, pracownik kancelarii szkoły itp). Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane oraz sposoby ich zabezpieczenia. W upoważnieniu określony jest rodzaj danych (podane konkretne zbiory) oraz zakres dostępu. Udostępnianie danych innym (np. opinii o uczniu) wymaga formy pisemnej, chyba że wynika z przepisów ustaw szczegółowych.

Powierzanie przetwarzania danych

Dane są udostępniane również instytucjom państwowym na podstawie ustaw szczególnych. W ten sposób gromadzone, przetwarzane i udostępniane są dane w Systemie Informacji Oświatowej, dane niezbędne do przeprowadzenia testów szóstoklasisty, egzaminów gimnazjalnych, maturalnych i innych. Powierzenie danych do obsługi innemu podmiotowi wymaga pisemnej umowy. Podmiot ten może przetwarzać dane wyłącznie w zakresie przewidzianym w umowie. Przed rozpoczęciem przetwarzania danych jest również obowiązany podjąć środki zabezpieczające zbiór danych oraz spełnić wymagania określone w przepisach art. 39a Ustawy.

Zgłaszanie zbiorów do GIODO

Administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi – „za wyjątkiem zbiorów przetwarzanych w związku z zatrudnieniem u nich, świadczeniem im usług na podstawie umów cywilnoprawnych, a także dotyczących osób u nich zrzeszonych lub uczących się" (zgodnie z art. 43.4 Ustawy).

Treść przepisów *Rozporządzenia Ministra Edukacji Narodowej z dnia 29 sierpnia 2014 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji* (Dz.U. 2014, poz. 1170) – które zastąpiło rozporządzenie Ministra Edukacji Narodowej i Sportu z dnia 19 lutego 2002 r. – wskazuje, że dane rodziców jako opiekunów prawnych są przyporządkowane konkretnym dzieciom, mają wobec nich charakter wtórny i są przetwarzane jedynie na potrzeby edukacji dzieci. **Zatem skoro w zbiorze przetwarzane są dane osób uczących się, a tak właśnie przepisy traktują dane dzieci uczęszczających do szkoły, to zbiór ten nie podlega obowiązkowi zgłoszenia do rejestracji.** Również zbiór danych rodziców i opiekunów prawnych dzieci – jedynie pomocniczy, ściśle związany ze zbiorem danych dzieci – jest traktowany jako zbiór zwolniony z obowiązku zgłoszenia do rejestracji.

Najczęściej rejestrowane przez Generalnego Inspektora są następujące zbiory danych prowadzone przez szkoły: rejestry uczniów realizujących obowiązek szkolny w innych placówkach, archiwa szkolne, zbiory dotyczące zamówień publicznych czy upoważnień do odbioru dzieci ze świetlicy szkolnej.

Jednym z najważniejszych obowiązków administratora danych jest zapewnienie, aby dane osobowe były przetwarzane zgodnie z prawem, w oparciu o właściwy przepis prawa (art. 23, 26, 27 Ustawy). Innymi słowy, przekazywanie danych osobowych przez administratorów danych przetwarzających dane osobowe innym podmiotom musi być zgodne z prawem, co oznacza, że konieczne jest istnienie podstawy prawnej odpowiedniej dla takiego działania.

Udostępnianie danych w określonej sytuacji jest uzależnione od spełnienia jednej z przesłanek legalności takiego działania określonych w przepisach Ustawy. W odniesieniu do tzw. zwykłych danych osobowych przesłanki legalności udostępniania (będącego formą przetwarzania) zostały określone w art. 23 ust. 1 Ustawy, zaś danych szczególnie chronionych – których katalog wymieniono w art. 27 ust. 1 – w ust. 2 tego aktu prawnego. Zarówno wobec danych zwykłych (wszystkich spoza ww. katalogu, tj. np. imienia, nazwiska, adresu), jak i danych szczególnie chronionych podstawę przetwarzania mogą stanowić przepisy innych aktów prawnych, przy czym w przypadku danych wrażliwych muszą być to przepisy rangi ustawowej, które dodatkowo gwarantują danym osobowym pełną ochronę. Tym samym

Ustawa odsyła do przepisów szczególnych, regulujących działalność określonych podmiotów i instytucji, wskazujących w jakich przypadkach i w jakim zakresie mogą one przetwarzać dane osobowe, aby obowiązki i uprawnienia nałożone na nie mocą tych przepisów mogły być realizowane.

Dopuszczalność udostępnienia danych w określonej sytuacji zależy bowiem od kategorii danych oraz od tego, jaki podmiot, na jakiej podstawie prawnej i w jakim celu wnioskuje o udostępnienie danych. Należy pamiętać, że w odniesieniu do określonych podmiotów oraz rodzaju danych istnieją szczególne – wobec Ustawy – regulacje prawne, które należy brać pod uwagę. Przepisy prawa mogą szczegółowo określać zasady udostępniania danych zawartych w określonym rodzaju dokumentacji. Właściwe przepisy prawa określają również kompetencje określonych instytucji lub osób do pozyskiwania danych, przy czym ze względu na to, że podmioty te realizują wiele różnych zadań lub potrzebują informacji dla różnych potrzeb, różne mogą być cele i podstawy prawne oraz uzasadnienie faktyczne żądania udostępniania danych.

W każdym konkretnym przypadku to administrator danych w oparciu o obowiązujące przepisy prawa oraz przy uwzględnieniu rodzaju danych osobowych, celu oraz uzasadnienia potrzeby posiadania danych przez podmiot, który występuje o ich udostępnienie, powinien dokonać oceny w zakresie dopuszczalności takiego udostępnienia. Podmiot występujący o udostępnienie określonych informacji powinien prawidłowo wskazać podstawę prawną upoważniającą go do uzyskania danych. W sytuacjach, gdy skierowane do administratora danych żądanie udzielenia danych osobowych budzi wątpliwości pod względem jego podstaw prawnych, dobrym rozwiązaniem może być zwrócenie się do wnioskodawcy z prośbą o wyjaśnienie tych wątpliwości.

Nie można mylić pojęć „udostępnienie danych” i „powierzenie przetwarzania danych”. Udostępnienie danych instytucjom państwowym na podstawie przepisów szczególnych powinno następować według wyżej określonych zasad. Natomiast jeśli chodzi o powierzenie przetwarzania, to istotne jest podkreślenie, że istotą tego rozwiązania (przewidzianego w art. 31 Ustawy) jest zlecenie wykonywania określonych operacji na danych osobowych innemu podmiotowi, który działa w tym zakresie nie we własnym imieniu, ale na rzecz i w imieniu administratora danych. Podstawą przekazania danych osobowych przez ich administratora innemu podmiotowi może być zawarta na piśmie pomiędzy nimi umowa powierzenia

przetwarzania danych. Jak wskazuje art. 31 ust. 2 Ustawy, taka umowa musi określać zakres i cel przetwarzania danych. Postanowienia stron dotyczące powierzenia przetwarzania danych mogą być inkorporowane do innej umowy łączącej te same strony. Podmiot, któremu przetwarzanie danych zostało powierzone na mocy art. 31 Ustawy, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36 – 39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a Ustawy. Należy również podkreślić, że w zakresie przestrzegania tych przepisów podmiot ten ponosi odpowiedzialność jak administrator danych (art. 31 ust. 3). Ponadto jest on związany w swojej działalności zakresem i celem przetwarzania wyznaczonym w przedmiotowej umowie. Innymi słowy oznacza to, ze podmiot, któremu powierzono przetwarzanie danych, może je przetwarzać wyłącznie w takim zakresie i celu, jaki został przewidziany w jej treści, a czyni to w imieniu i na rzecz administratora, który powierzając dane do przetwarzania, nie wyzbywa się statusu podmiotu decydującego o celach i środkach przetwarzania danych osobowych. Z perspektywy dyrektora szkoły bardzo ważne jest to, że w takiej sytuacji nadal spoczywa na nim odpowiedzialność za przestrzeganie przepisów ustawy, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.

W szkołach może dochodzić do powierzenia przetwarzania danych np. w sytuacji zlecenia podmiotom zewnętrznym wykonania legitymacji służbowych nauczycieli lub zlecenia wyspecjalizowanym podmiotom zewnętrznym obsługi informatycznej dzienników elektronicznych. W takich sytuacjach dochodzi do udostępnienia danych innym podmiotom na zasadzie powierzenia przetwarzania danych.

Czy należy zgłaszać do GIODO następujące zbiory: podania o przyjęcie do pracy z listami motywacyjnymi i/lub CV od osób, które nie zostały zatrudnione; teczki akt osobowych pracowników, którzy nie są już pracownikami; arkusze ocen uczniów, którzy odeszli ze szkoły w trakcie nauki (np. w IV klasie – nie są ani uczniami, ani absolwentami); arkusze absolwentów; księgę absolwentów; dzienniki archiwalne, w których są dane absolwentów?

Podania o przyjęcie do pracy z listami motywacyjnymi i/lub CV od osób, które nie zostały zatrudnione: zbiory zawierające dane kandydatów do pracy (zatrudnionych i niezatrudnionych) prowadzone w związku z rekrutacją u danego administratora danych **nie muszą być zgłaszane** do GIODO. Należy pamiętać jednak o przestrzeganiu zasad legalności – podstawa prawna, celowość i ograniczenie czasowe w kontekście przechowywania ofert osób niezatrudnionych.

Teczki akt osobowych pracowników, którzy nie są już pracownikami: zbiory zawierające dane byłych pracowników administratora danych przetwarzanych w związku z byłym zatrudnieniem **nie muszą być zgłaszane** do GIODO.

Arkusze ocen uczniów, którzy odeszli ze szkoły w trakcie nauki (np. w IV klasie – nie są ani uczniami, ani absolwentami), arkusze absolwentów, księga absolwentów, dzienniki archiwalne, w których są dane absolwentów: zbiory zawierające dane absolwentów lub innych byłych uczniów **nie muszą być zgłaszane** do GIODO, o ile zostały one stworzone z danych pozyskanych (wytworzonych) w związku z nauką uczniów w danej szkole. Nie ma obowiązku rejestrowania danych byłego ucznia pozostających w dzienniku czy arkuszu, ponieważ znalazły się one tam zgodnie z przepisami prawa. **Rejestrowane są natomiast zbiory absolwentów (zwłaszcza szkół wyższych) przetwarzane np. w związku z monitorowaniem karier czy w celach informacyjno-promocyjnych**, a więc gdy nie chodzi o dokumentację powstałą podczas nauki szkolnej.

Czy prowadzenie przez szkołę elektronicznych dzienników lekcyjnych (tzw. e-dzienników) nie narusza prawa do ochrony danych osobowych uczniów?

Nie, gdyż prowadzenie dzienników lekcyjnych, w których zawarte są informacje o uczniach, wynika z przepisów prawa, a forma – elektroniczna czy papierowa – jest jedynie kwestią techniczną.

Ustawa o ochronie danych osobowych (Dz.U. 2002 nr 101, poz. 926, z późn. zm.) określa jedynie ogólne zasady przetwarzania danych osobowych, zaś gdy istnieją inne – szczególne wobec Ustawy przepisy prawa – należy je stosować w pierwszej kolejności. Zakres informacji o uczniach, które mogą być gromadzone przez szkoły, określa rozporządzenie sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz.U. 2014, poz. 1170), wydane na podstawie ustawy o systemie oświaty (Dz.U. 1991 nr 95, poz. 425).

Zgodnie z § 7 ust. 1 tego rozporządzenia szkoła prowadzi dla każdego oddziału dziennik lekcyjny, w którym dokumentuje się przebieg nauczania w danym roku szkolnym. Do dziennika lekcyjnego wpisuje się w porządku alfabetycznym – lub innym ustalonym przez dyrektora szkoły – nazwiska i imiona uczniów, daty i miejsca urodzenia oraz adresy ich zamieszkania, imiona i nazwiska rodziców (prawnych opiekunów) i adresy ich zamieszkania, a także tygodniowy plan zajęć edukacyjnych, oznaczenie realizowanych programów nauczania zawartych w szkolnym zestawie programów nauczania dla danego oddziału oraz imiona i nazwiska nauczycieli prowadzących poszczególne zajęcia. W dzienniku lekcyjnym odnotowuje się obecność uczniów na zajęciach edukacyjnych oraz wpisuje się tematy przeprowadzonych zajęć, oceny i zaliczenia uzyskane przez uczniów z poszczególnych zajęć edukacyjnych, oceny zachowania, a także przeprowadzone hospitacje zajęć, które nauczyciel potwierdza podpisem (§ 7 ust. 2 i 3).

Z kolei możliwość prowadzenia dzienników lekcyjnych w formie elektronicznej przewidziana jest w *Rozporządzeniu Ministra Edukacji Narodowej z dnia 16 lipca 2009 r. zmieniającego rozporządzenie w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji* (Dz.U. 2009 nr 116, poz. 977; § 20a ust. 1). Prowadzenie dziennika elektronicznego jest więc alternatywą do dziennika w formie tradycyjnej, papierowej. Co prawda za zgodą organu prowadzącego szkołę dzienniki lekcyjne mogą być prowadzone wyłącznie w formie elektronicznej, ale wówczas szkoła (jako administrator

danych) ma obowiązek zastosowania szeregu wymogów dotyczących prowadzenia takich dzienników. Związana jest z tym m.in. konieczność zachowania kontroli nad tym, kto ma dostęp do danych stanowiących dziennik elektroniczny oraz zabezpieczenia ich przed dostępem osób nieuprawnionych, przed zniszczeniem, uszkodzeniem lub utratą (§ 20a ust. 3).

Forma, w jakiej prowadzony jest dziennik lekcyjny – czy to papierowa, czy elektroniczna – jest więc jedynie kwestią techniczną, pozostawioną szkołom do wyboru. Istotne jest natomiast to, że informacje o uczniach zawarte w dziennikach lekcyjnych stanowią dane osobowe i mogą być wykorzystywane przez szkołę (gromadzone, przechowywane, udostępniane) tylko w zakresie stanowionym przez powyższe przepisy prawa.

Niemniej jednak bardzo ważne jest, aby przetwarzanie danych osobowych w dziennikach elektronicznych odbywało się przy zapewnieniu odpowiednich środków bezpieczeństwa danych osobowych. Dyrektor szkoły musi zwrócić na to uwagę również wtedy, gdy dzienniki elektroniczne są prowadzone przez podmioty zewnętrzne.

Czy od rodziców zapisujących dziecko do świetlicy szkolnej można żądać podania takich danych, jak ich miejsce zatrudnienia, stanowisko oraz wynagrodzenie?

Nie, gdyż przepisy, na podstawie których działają placówki oświatowe, nie dają podstawy do pozyskiwania takich informacji, a poza tym byłyby one zbędne dla realizacji celu, jakim jest zapisanie dziecka do świetlicy szkolnej.

Przetwarzanie danych osobowych przez placówki oświatowe odbywa się przede wszystkim na podstawie przepisów szczególnych w stosunku do ustawy o ochronie danych osobowych, zwłaszcza zaś ustawy systemie oświaty oraz wydanych na jej podstawie aktów wykonawczych, m.in. rozporządzenia w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji.

Rozporządzenie to stanowi, jakiego rodzaju dokumentację prowadzi szkoła i jakie dane osobowe ona zawiera.

Do księgi ewidencji dzieci podlegających obowiązkowi przygotowania przedszkolnego i obowiązkowi szkolnemu, zamieszkałych w obwodzie szkoły, wpisuje się według roku

urodzenia: imię (imiona) i nazwisko, datę i miejsce urodzenia, numer PESEL oraz adres zamieszkania dziecka, a także imiona i nazwiska rodziców (prawnych opiekunów) oraz adresy ich zamieszkania (§ 3a ust. 1 i 2 pkt 1, § 3b ust. 1 i 2).

Z kolei do księgi uczniów wpisuje się imię (imiona) i nazwisko, datę i miejsce urodzenia, numer PESEL oraz adres zamieszkania ucznia, imiona i nazwiska rodziców (prawnych opiekunów) i adresy ich zamieszkania, a także datę przyjęcia ucznia do szkoły oraz klasę, do której go przyjęto. Odnotowuje się w niej również datę ukończenia szkoły albo datę i przyczynę opuszczenia szkoły przez ucznia (§ 4 ust. 1 i 2).

Omawiane rozporządzenie stanowi też, jakie dane powinny być zawarte w dzienniku lekcyjnym (zgodnie z § 7 ust. 1 są to m.in.: nazwiska i imiona uczniów, daty i miejsca urodzenia oraz adresy ich zamieszkania, imiona i nazwiska rodziców lub prawnych opiekunów i adresy ich zamieszkania), a jakie w dzienniku zajęć w świetlicy (są to m.in.: imiona i nazwiska uczniów korzystających ze świetlicy, klasa, do której uczęszczają, czy odnotowanie obecności uczniów na poszczególnych godzinach zajęć).

Z przytoczonych powyżej przepisów nie wynika, by placówka oświatowa na potrzeby zapisania dziecka do świetlicy szkolnej mogła żądać od rodziców takich danych, jak ich miejsce zatrudnienia, stanowisko oraz wynagrodzenie. Tym samym brak jest podstawy prawnej do przetwarzania (m.in. gromadzenia) tego typu danych osobowych. Ich pozyskiwanie może zaś prowadzić do naruszenia art. 26 ustawy o ochronie danych osobowych, zgodnie z którym administrator danych (w tym przypadku szkoła) przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dotyczą dane, a w szczególności jest obowiązany zapewnić, aby dane te były: przetwarzane zgodnie z prawem (pkt 1), zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami (pkt 2), merytorycznie poprawne i adekwatne do celów, w jakich są przetwarzane (pkt 3).

Na konieczność stosowania tzw. zasady adekwatności przy przetwarzaniu danych osobowych wskazał również Wojewódzki Sąd Administracyjny, który w wyroku z 1 grudnia 2005 r. (sygn. akt II SA/Wa 917/2005) orzekł, że „Adekwatność danych w stosunku do celu ich przetwarzania powinna być rozumiana jako równowaga pomiędzy uprawnieniem osoby do dysponowania swymi danymi a interesem administratora danych. Równowaga będzie

zachowana, jeżeli administrator zażąda danych tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu, w jakim dane są przez niego przetwarzane".

Szkoła pozostaje administratorem danych, nawet gdy dziennik elektroniczny prowadzi podmiot zewnętrzny.

Czy placówki oświatowe są zobowiązane do zawarcia pisemnej umowy powierzenia przetwarzania danych osobowych z przedsiębiorcą, który udostępnia im system informatyczny do prowadzenia e-dzienników?

Tak, gdyż ustawa o ochronie danych osobowych wymaga, aby umowa powierzenia przetwarzania danych była zawarta w formie pisemnej.

Na podstawie art. 31 ust. 1 ustawy o ochronie danych osobowych administrator danych (w tym np. placówka oświatowa) może powierzyć przetwarzanie danych innemu podmiotowi, w drodze umowy zawartej na piśmie. Niezbędnymi elementami tej umowy jest określenie celu, w jakim podmiot, któremu powierzono przetwarzanie danych, może je przetwarzać, oraz zakresu danych powierzonych do przetwarzania. Podmiot ten może bowiem przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie. Powierzenie przetwarzania danych na podstawie umowy, o której stanowi art. 31 ustawy, w określonym w niej celu jest działaniem prawnie dopuszczalnym i nie stanowi nieuprawnionego udostępnienia danych przez ich administratora innemu podmiotowi.

Placówki oświatowe mogą prowadzić dzienniki elektroniczne (e-dzienniki) na podstawie rozporządzenia w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji. Jeśli placówka oświatowa korzysta z oferowanego jej przez przedsiębiorcę systemu informatycznego w celu prowadzenia elektronicznych dzienników, w których przetwarzane są dane osobowe uczniów, ich przedstawicieli ustawowych oraz nauczycieli, powinna zawrzeć z nim pisemną umowę powierzenia przetwarzania danych osobowych. Umowa udzielenia licencji na korzystanie z systemu informatycznego zawarta z chwilą otrzymania przez placówkę oświatową kodu dostępu do systemu informatycznego nie spełnia wymogów z art. 31 ustawy o ochronie danych osobowych.

Mimo że placówka oświatowa powierza przedsiębiorstwu przetwarzanie danych osobowych w celu wykonania umowy, to brak formy pisemnej dyskwalifikuje ją jako umowę powierzenia z art. 31 ww. ustawy. Hostingowi nie wystarczy także pisemna umowa, jeśli nie zawiera ona postanowień, z których wynikałoby, że na ich podstawie powierzono przetwarzanie danych osobowych w celu wykonania tej umowy.

W związku z powyższym placówki oświatowe są zobowiązane do podpisania umowy powierzenia przetwarzania danych z przedsiębiorcą, który udostępnia im system informatyczny do prowadzenia e-dzienników.

Czy skarbnik gminy – organu prowadzącego kilka placówek oświatowych – może mieć dostęp do operacji finansowych dokonywanych na kontach tych placówek?

Tak, gdyż wynika to z przepisów ustawy o systemie oświaty, która uprawnia podmiot prowadzący placówkę oświatową do kontroli jej działalności w zakresie m.in. spraw finansowych.

Bazy danych oświatowych prowadzone przez szkoły i inne placówki oświatowe obejmują m.in. zbiory danych o nauczycielach, wychowawcach i innych pracownikach pedagogicznych. Zbiór ten zawiera dane obejmujące ich numery PESEL, płeć, rok urodzenia, formy i wymiar zatrudnienia, stopień awansu zawodowego, wykształcenie, przygotowanie pedagogiczne, formę kształcenia i doskonalenia, sprawowane funkcje i zajmowane stanowiska, rodzaje prowadzonych zajęć albo przyczyn nieprowadzenia zajęć, stażu pracy, wysokości wynagrodzenia, z wyszczególnieniem jego składników, wysokości dodatków, o których mowa w art. 54 ust. 3 i 5 Karty Nauczyciela (art. 3 ust. 4 pkt 1 w zw. z art. 4 ust. 1 *Ustawy z dnia 19 lutego 2004 r. o systemie informacji oświatowej*, Dz.U. 2004 nr 49, poz. 463).

Zgodnie zaś z art. 5 ust. 7 ustawy o systemie oświaty organ prowadzący szkołę lub placówkę odpowiada za jej działalność. Do zadań tego organu należy zapewnienie obsługi administracyjnej, finansowej i organizacyjnej szkoły lub placówki (art. 5 ust. 7 pkt 3). Na podstawie art. 34a ust. 1 ustawy o systemie oświaty organ prowadzący szkołę lub placówkę sprawuje nadzór nad jej działalnością w zakresie spraw finansowych i administracyjnych, z uwzględnieniem odrębnych przepisów. W powyższym zakresie nadzorowi podlega w

szczególności prawidłowość dysponowania przyznanymi szkole lub placówce środkami budżetowymi oraz pozyskanymi przez nie środkami pochodzącymi z innych źródeł, a także gospodarowania mieniem, przestrzeganie obowiązujących przepisów dotyczących bezpieczeństwa i higieny pracy pracowników i uczniów, przestrzeganie przepisów dotyczących organizacji pracy szkoły i placówki (art. 34a ust. 2).

Jednocześnie należy zauważyć, że ustawa o ochronie danych osobowych wprowadziła zasadę, według której do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych. Administrator danych, czyli podmiot decydujący o celach i środkach przetwarzania danych (np. szkoła, placówka oświatowa, urząd gminy), ponosi bowiem odpowiedzialność za bezpieczeństwo przetwarzanych danych osobowych, w tym m.in. za ich udostępnienie osobom nieupoważnionym. Upoważnienie powinno być udzielone nie tylko osobom, które zostały bezpośrednio zatrudnione w celu przetwarzania danych, lecz także osobom, które mogą w takim przetwarzaniu uczestniczyć. Należy przy tym podkreślić, że administrator danych powinien nadać upoważnienie do przetwarzania danych jedynie tym osobom, które w ramach wykonywania powierzonych im obowiązków służbowych mają dostęp do danych osobowych.

W upoważnieniu powinny być określone: nazwa (nazwisko) i adres administratora danych, osoba upoważniona do przetwarzania danych osobowych, data nadania i, jeżeli upoważnienie jest przyznawane na czas określony, ustania oraz zakres upoważnienia do przetwarzania danych osobowych (por. Drozd, 2004).

W związku z powyższym skarbnik gminy i organu prowadzącego kilka placówek oświatowych może mieć dostęp do operacji finansowych dokonywanych na ich kontach, ale po otrzymaniu stosownego upoważnienia od każdej takiej placówki, będącej administratorem danych przetwarzanych w prowadzonych przez nie zbiorach.

Czy praktyka stosowana w szkołach, polegająca na publicznym wyczytywaniu nazwisk i podawaniu informacji o uczniach podczas zebrań rodziców, jest zgodna z ustawą o ochronie danych osobowych?

Taka praktyka wymaga dokonania uzgodnień między dyrektorem szkoły, nauczycielami i rodzicami czy opiekunami prawnymi uczniów, którzy do momentu osiągnięcia pełnoletności

przez dzieci muszą wyrazić zgodę na wykorzystywanie ich danych osobowych. Nie ma bowiem przepisów regulujących takie sprawy, jak np. publiczne odczytywanie informacji o uczniach, podawanie frekwencji lub średniej ocen czy sporządzanie lub upublicznianie rankingu uczniów. To już bardziej kwestia tradycji i woli rodziców czy opiekunów prawnych oraz zdroworozsądkowego podejścia do sprawy. Zbyt formalistyczne traktowanie zagadnienia nie jest potrzebne. Jak bowiem wówczas przeprowadzać np. konkursy, rozgrywki czy inne formy współzawodnictwa, u podstaw których leży podawanie wyników, czyli ustalanie kolejności miejsc zajętych przez konkretne osoby?

Niemniej jednak o uzgodnionych i przyjętych w danej szkole czy placówce procedurach należy poinformować uczniów i rodziców oraz uzyskać zgodę tych ostatnich na taką formę przetwarzania danych. Choć ustawa nie wymaga zgody pisemnej, to warto o taką poprosić, choćby do celów dowodowych w przypadku np. skargi na nieuprawnione wykorzystywanie danych. Na co dzień zwykle nie zwraca się uwagi na takie sytuacje: podczas szkolnych imprez dzieci bywają fotografowane, rodzice utrwalają obraz kamerami, następnie zdjęcia są wywieszane w gablotkach, na tablicach, umieszczane na stronie www. Na początku roku szkolnego trzeba uzgodnić z rodzicami zasady postępowania, m.in. upubliczniania zdjęć jednej osoby (nie możemy zabronić pokazywania danego zdjęcia grupowego, gdyż wszyscy, którzy się na nim znajdują, mają do niego prawo). Ustawa o prawie autorskim i prawach pokrewnych stanowi, że zezwolenia nie wymaga rozpowszechnianie wizerunku osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza.

Blokowanie publikowania danych w formie gazetki ściennej, kroniki itp. byłoby zatem nielogiczne. Niech każdy odpowie sobie na pytanie, czy chciałby, aby przestały istnieć szkolne kroniki upamiętniające najważniejsze wydarzenia z historii danej placówki i życia jej uczniów. Ważne jest, aby dbając o prywatność osób, zachowywać zdrowy rozsądek.

Czy dyrektor szkoły może przetwarzać posiadane przez szkołę dane osobowe na potrzeby złożenia pozwu do sądu dla nieletnich?

Tak, bowiem takie uprawnienie wynika z przepisów prawa, zwłaszcza z *Ustawy z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich* (Dz.U. 1982 nr 35, poz. 228).

Zgodnie z ustawą o ochronie danych osobowych wykonywanie jakichkolwiek operacji na danych osobowych jest dopuszczalne m.in. wówczas, gdy zezwalają na to inne – szczególne względem tej ustawy – przepisy prawa (art. 23 ust. 1 pkt 2).

Zgodnie z treścią § 4 ust. 1 i 2 rozporządzenia w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji szkoła prowadzi księgę uczniów, do której wpisuje się:

- imię (imiona) i nazwisko ucznia,
- datę i miejsce urodzenia ucznia,
- adres zamieszkania ucznia,
- imiona i nazwiska rodziców (prawnych opiekunów),
- adresy zamieszkania rodziców (prawnych opiekunów),
- datę przyjęcia ucznia do szkoły,
- klasę, do której ucznia przyjęto,
- datę ukończenia szkoły albo datę i przyczynę opuszczenia szkoły przez ucznia.

Do zadań dyrektora szkoły należy natomiast sprawowanie opieki nad dziećmi i młodzieżą uczącą się w szkole (art. 7 ust. 1 zd. 2 Karty Nauczyciela). Jest on także odpowiedzialny za dydaktyczny i wychowawczy poziom szkoły (art. 7 ust. 2 pkt 1 Karty Nauczyciela).

Z kolei art. 4 § 1 ustawy o postępowaniu w sprawach nieletnich stanowi, że każdy, kto stwierdzi istnienie okoliczności świadczących o demoralizacji nieletniego, w szczególności naruszanie zasad współżycia społecznego, popełnienie czynu zabronionego, systematyczne uchylanie się od obowiązku szkolnego lub kształcenia zawodowego, używanie alkoholu lub innych środków w celu wprowadzenia się w stan odurzenia, uprawianie nierządu, włóczęgostwo, udział w grupach przestępczych, ma społeczny obowiązek odpowiedniego przeciwdziałania temu, a przede wszystkim zawiadomienia o tym rodziców lub opiekuna nieletniego, szkoły, sądu rodzinnego, policji lub innego właściwego organu.

Biorąc pod uwagę powyższe przepisy, należy uznać, że dyrektor szkoły ma prawo wykorzystać dane osobowe zawarte w księdze uczniów w celu złożenia wniosku do sądu dla nieletnich. Takie postępowanie nie narusza przepisów ustawy o ochronie danych osobowych.

Odrębną kwestią, pozostającą poza kompetencjami GIODO, jest ocena zasadności skierowania wniosku do sądu dla nieletnich.

Aktami prawnymi określającymi kompetencje dyrektora szkoły oraz wskazującymi, w jakim zakresie szkoła może przetwarzać dane osobowe uczniów, są m.in.: ustawa o systemie oświaty, *Ustawa z dnia 26 stycznia 1982 r. Karta Nauczyciela*, rozporządzenie w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji, *Ustawa z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich*.

Czy szkoła posiadająca rejestr uczniów realizujących obowiązek szkolny w innych szkołach powinna zgłosić taki zbiór danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych?

Tak, gdyż zbiór ten nie dotyczy osób uczących się w tej szkole, a tylko taki jest zwolniony z rejestracji.

Zgodnie z art. 40 ustawy o ochronie danych osobowych administrator danych jest obowiązany zgłosić zbiór danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (GIODO), chyba że zachodzi jedna z przesłanek określonych w art. 43 ust. 1 pkt 1–11 ustawy. W myśl wskazanego w tym przepisie pkt 4 z obowiązku rejestracji zbioru danych zwolnieni są m.in. administratorzy danych prowadzący zbiory danych uczących się u nich osób. Natomiast jeśli szkoła przetwarza (np. tylko przechowuje) zbiory danych osób, które *de facto* uczą się w innych placówkach oświatowych, wówczas wskazana wyżej przesłanka zwolnienia z rejestracji nie ma zastosowania. Tym samym takie zbiory danych osobowych powinny zostać zarejestrowane u Generalnego Inspektora Ochrony Danych Osobowych.

Czy nauczyciele mogą wyrazić zgodę na to, by przedstawiciele firmy marketingowej w trakcie prowadzonych lekcji gromadzili informacje o uczniach i ich rodzicach (imieniu, nazwisku, numerze telefonu) w celu prowadzenia akcji marketingowej?

Nie, gdyż zgodę na wykorzystywanie danych osobowych uczniów w celach marketingowych mogą wyrazić tylko oni sami, a jeśli są niepełnoletni, to muszą to zrobić ich rodzice (opiekunowie prawni).

Szkoła, poza wypełnianiem swoich dydaktyczno-wychowawczych obowiązków, powinna jednocześnie czuwać nad zapewnieniem ochrony prywatności dzieci.

Trzeba zauważyć, że zgoda dyrektora szkoły czy poszczególnych nauczycieli lub wychowawców na przetwarzanie danych osobowych dzieci lub ich rodziców nie jest wystarczająca, by można było mówić o legalnym wykorzystywaniu tych danych. Aby można było mówić o działaniu legalnym, konieczne byłoby uzyskanie zgody rodziców czy opiekunów prawnych dzieci. Należy podkreślić, że zgoda na przetwarzanie danych osobowych wyrażona przez osoby małoletnie pozostaje bezskutecznym oświadczeniem woli do czasu jej potwierdzenia przez rodziców czy też opiekunów prawnych. Taka zgoda jest pozbawiona mocy prawnej również w świetle obowiązujących przepisów *Ustawy z dnia 25 lutego 1964 r. Kodeks rodzinny i opiekuńczy* (Dz.U. 1964 nr 9, poz. 59).

Jeśli nawet dane osobowe uczniów nie zostają w tej sytuacji udostępnione bezpośrednio przez pracowników szkoły, niemniej jednak wskutek ich nieprawidłowego zachowania, dochodzi do pozyskania danych osobowych uczniów w zakresie, który pozwala przedstawicielowi firmy na dotarcie z ofertą marketingową do ich rodziców, wzbudzając w pełni uzasadnione poczucie zagrożenia prywatności tych osób.

Dlatego też nauczyciele nie powinni uciekać się do metod, których zastosowanie naraża na niebezpieczeństwo zarówno prywatność dzieci, jak i ich rodziców. **Nauczyciele nie mają prawa udostępniać danych uczniów z dziennika zajęć lekcyjnych lub innych posiadanych przez szkołę dokumentów oraz nie mogą wyrażać skutecznej zgody na przetwarzanie danych w imieniu dzieci.**

Czy publikowanie na ogólnej dostępnej stronie internetowej szkoły takich danych jak imiona i nazwiska uczniów przydzielonych do grup zdających egzamin klasyfikacyjny jest zgodne z przepisami ustawy o ochronie danych osobowych?

Tak, publikowanie na ogólnie dostępnej stronie internetowej szkoły imion i nazwisk uczniów przydzielonych do grup zdających egzamin klasyfikacyjny może się odbywać wyłącznie pod warunkiem, że rodzice lub opiekunowie prawni uczniów, których dotyczą dane, wyrażą na to pisemną zgodę.

Przetwarzanie danych jest dopuszczalne m.in. w sytuacji, gdy osoba, której dotyczą dane, wyrazi na to zgodę lub gdy przetwarzanie jest niezbędne do zrealizowania uprawniania lub spełnienia obowiązku wynikającego z przepisu prawa (ustawa o ochronie danych osobowych). Ponieważ ustawa ta określa jedynie ogólne zasady przetwarzania danych, to w wielu konkretnych sprawach zastosowanie znajdują przepisy szczególne. W opisanym przypadku przesłanek do publikacji danych osobowych należy szukać w przepisach, które wiążą się ściśle z przetwarzaniem danych osobowych w szkole:

- *Rozporządzenie Ministra Edukacji Narodowej i Sportu z dnia 19 lutego 2002 r. w sprawie sposobu przeprowadzania przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji* (Dz.U. 2002 nr 23, poz. 225) oraz
- *Rozporządzenie Ministra Edukacji Narodowej i Sportu z dnia 20 lutego 2004 r. w sprawie warunków i trybu przyjmowania uczniów do szkół publicznych oraz przechodzenia z jednych typów szkół do innych* (Dz.U. 2004 nr 26, poz. 232).

Żadne z tych rozporządzeń nie wskazuje jednoznacznie obowiązku publikacji na stronie internetowej imienia i nazwiska osoby przydzielonej do grupy uczniów zdających egzamin klasyfikacyjny. Nie ma więc podstaw prawnych, by publikować dane osobowe, powołując się na obowiązek wynikający z przepisów. Jednak można je upubliczniać w sytuacji gdy osoba, której dane dotyczą, wyrazi na to zgodę. Ponieważ w opisanej sprawie mamy do czynienia z dziećmi, a więc osobami niepełnoletnimi, które przed ukończeniem 13. roku życia nie mają pełnej zdolności do czynności prawnych, ich zgoda nie byłaby ważna (skuteczna). Niemniej w ich imieniu decyzję o upublicznieniu danych osobowych poprzez publikację na stronie internetowej szkoły mogą wyrazić ich rodzice lub opiekunowie prawni.

Pozyskanie takiej zgody wypełniłoby warunek legalizujący upublicznienie danych w internecie.

Czy szkoły mogą przetwarzać dane biometryczne – odciski palców?

Nie ma przepisu, który zezwalałby szkołom na pozyskiwanie od uczniów i pracowników odcisków palców w celu zapewnienia kontroli osób wchodzących do budynku. Nie uzasadniają tego nawet względy bezpieczeństwa oraz wyrażenie zgody przez zainteresowane osoby.

To, jakie dane szkoły mogą pozyskiwać od swoich pracowników oraz uczniów, regulują odpowiednio przepisy prawa pracy oraz przepisy branżowe opisujące funkcjonowanie placówek oświatowych. Żadne z nich nie zezwalają tym podmiotom na przetwarzanie, a więc m.in. pozyskiwanie i gromadzenie, odcisków palców uczniów oraz nauczycieli i innych pracowników, np. w celu kontroli dostępu do budynku.

Takie postępowanie prowadzi do naruszenia zasady adekwatności ustanowionej w ustawie o ochronie danych osobowych, zgodnie z którą administrator danych, czyli w tym przypadku szkoła, nie powinien pozyskiwać danych osobowych ponad miarę, lecz jedynie te, które są niezbędne dla zrealizowania celów. Tymczasem kontrolę tego, kto wchodzi do budynku, można zapewnić w inny sposób lub za pomocą innych technik, np. poprzez wprowadzenie kart magnetycznych. Pozyskiwanie takich danych od uczniów i pracowników szkoły stanowi zbyt dużą ingerencję w ich prywatność. Naczelny Sąd Administracyjny w wyroku z dnia 1 grudnia 2009 r. również orzekł, że pozyskiwanie na potrzeby ewidencji czasu pracy odcisku palca pracowników, nawet za ich zgodą, jest niedozwolone. Dopuszczalne byłoby to jedynie wówczas, gdyby w ten sposób pracodawca chciał ograniczyć dostęp niektórych osób do szczególnie istotnych stref (GIODO, b.r.).

Bibliografia i podstawa prawna

Drachal H., (2010), *Twoje dane pod ochroną – z dyr. Wojciechem Rafałem Wiewiórskim, Generalnym Inspektorem Ochrony Danych Osobowych, rozmawia Halina Drachal*, „Głos Nauczycielski", nr 43, s. 9.

Drozd A., (2004), *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Warszawa: Wydawnictwo Prawnicze LexisNexis.

GIODO, (b.r.), *Dla TVP Szczecin o wykorzystywaniu odcisków palców przez szkoły, 15.01.2010 r.* (źródło internetowe: http://giodo.gov.pl/1520001/id_art/3287/j/pl, dostęp dn. 29.08.2014). Roszak A., (2013), *Konsekwencje naruszenia ustawy o ochronie danych osobowych* (dostęp dn. 29.09.2014).

Securelist, (b.r.), *Skype i bezpieczeństwo sieci korporacyjnych* (dostęp dn. 29.09.2014).

Rozporządzenie Ministra Edukacji Narodowej z dn. 29 sierpnia 2014 r. w sprawie sposobu prowadzenia przez publiczne przedszkola, szkoły i placówki dokumentacji przebiegu nauczania, działalności wychowawczej i opiekuńczej oraz rodzajów tej dokumentacji (Dz.U. 2014 poz. 1170).

Ustawa z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (Dz.U. 2012, nr 1015 z późn. zm.).

Ustawa z dnia 7 września 1991 r. o systemie oświaty (tekst jednolity: Dz.U. 2004, nr 256, poz. 2572).

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. 2014, poz. 1182).

Załączniki

Załącznik nr 1. Przykładowe upoważnienie udzielane pracownikowi[17] przez dyrektora szkoły

UPOWAŻNIENIE nr 1/DO/2014

z 1 września 2013 r.

Na podstawie *Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 2002 nr 101, poz. 926 i nr 153, poz. 1271)* oraz *z 2004 r. (Dz.U. 2004 nr 25, poz. 219 i nr 33, poz. 285)*

upoważniam Panią/Pana Agnieszkę Nowak

/imię i nazwisko/

zatrudnioną w Szkole Podstawowej nr 5 w Szczytnie, ul. Batorego 6, 05-340 Szczytno

/nazwa placówki/

na okres od 1 września 2014 do 31 sierpnia 2015 roku do tworzenia i przetwarzania następujących zbiorów:

Zbiór 2 – Dzienniki zajęć obowiązkowych i dodatkowych;
Zbiór 5 – Arkusze ocen;
Zbiór 9 – Zgody;
Zbiór 27 – System edPlan.

W związku z dostępem do zbioru nr 27 ustalam dane dostępowe do zbioru danych gromadzonych w systemie EdPlan:

Login: agn_now_76
Hasło: bgt5&YHN

Ponadto upoważniam Panią do przetwarzania danych osobowych zawartych w zbiorach:

Zbiór 11 – Zaświadczenia z PPP i inne orzeczenia i opinie

Ustalam Pani *nazwę użytkownika*: agn.noW i *hasło*: nW26Ag oraz upoważniam do logowania się na stanowisku komputerowym do dyspozycji nauczycieli w pokoju nauczycielskim.

_____

/podpis dyrektora szkoły/

[17] Aby upoważnienie było zrozumiałe dla pracownika, musi on być wcześniej przeszkolony i zapoznany ze zbiorami i procedurami obowiązującymi w danej szkole.

Załącznik nr 2. Przykładowy wykaz zbiorów w szkole podstawowej

Zbiór 1: Ewidencja osób zatrudnionych przy przetwarzaniu danych osobowych a) Segregator *Dane osobowe* b) Skoroszyt *Rejestr i upoważnienia wydane przez dyrektora* c) Skoroszyt *Wewnątrzszkolny system gromadzenia i przetwarzania danych osobowych*
Zbiór 2: Dzienniki zajęć obowiązkowych i dodatkowych a) Dzienniki zajęć lekcyjnych i pozalekcyjnych b) Teczki wychowawców (informacje o uczniach, kontakt z rodzicami, informacje o rodzinie – kwestionariusze, notatki z rozmów z rodzicami i uczniami, usprawiedliwienia nieobecności uczniów na zajęciach) c) Zestawienia klasyfikacyjne i statystyczne
Zbiór 3: Księga uczniów
Zbiór 4: Rejestry a) Rejestr wydanych legitymacji szkolnych b) Rejestr wydanych kart rowerowych i motorowerowych c) Rejestr wypadków d) Rejestr absolwentów
Zbiór 5: Arkusze ocen a) Arkusze ocen uczniów będących uczniami szkoły b) Arkusze archiwalne
Zbiór 6: Rekrutacja uczniów a) Podania o przyjęcie do szkoły b) Podania archiwalne
Zbiór 7: Kształcenie specjalne a) Zbiór orzeczeń o potrzebie kształcenia specjalnego b) Zbiór opinii z poradni psychologiczno-pedagogicznych c) Indywidualne programy edukacyjno-terapeutyczne d) Segregatory dokumentacji indywidualnego przebiegu nauczania ucznia ze szczególnymi potrzebami edukacyjnymi
Zbiór 8: System Informacji Oświatowej a) Segregator SIO (kopie elektroniczne baz danych, kopie przesłanych dokumentów, raporty) b) Dane do wprowadzania SIO (zestawienia, notatki wychowawców) c) Skoroszyt upoważnień do SIO (wnioski, nadanie uprawnień, zmiany, hasła) itp.
Zbiór 9: Segregator *Zgody* a) Zbiór zgód dotyczących wyrażenia zgody lub nie na uczęszczanie na lekcje religii b) Zbiór zgód dotyczących zajęć wychowania do życia w rodzinie c) Zbiór zgód rodziców na publikację zdjęć i informacji w Internecie oraz środkach masowego przekazu d) Zbiór zgód dotyczących udziału w programach ogólnoszkolnych (np. szklanka mleka, owoce w szkole) e) Zbiór innych zgód
Zbiór 10: Segregator *Decyzje dyrektora szkoły* (*Ewidencja decyzji*)

a) Skoroszyt decyzji dotyczących zwolnień z obowiązkowych zajęć WF b) Skoroszyt decyzji dotyczących odroczenia obowiązku szkolnego c) Skoroszyt decyzji dotyczących skreślenia z listy uczniów d) Inne decyzje wydawane w trybie administracyjnym
Zbiór 11: Segregator *Stypendia* a) Wnioski o przyznanie stypendiów szkolnych i specjalnych wraz z załącznikami b) Decyzje c) Listy wypłat d) Zestawienia i raporty e) Potwierdzenia złożonych dokumentów
Zbiór 12: Segregator *Dofinansowanie zakupu podręczników* a) Wnioski o przyznanie dofinansowania wraz z załącznikami b) Decyzje c) Listy wypłat d) Zestawienia i raporty e) Potwierdzenia złożonych dokumentów
Zbiór 13: Dofinansowanie posiłków a) Decyzje o przyznaniu dofinansowania b) Listy uczniów korzystających z posiłków c) Rozliczenie miesięczne wydanych posiłków
Zbiór 14: Kontrola wewnętrzna a) Skoroszyty i dokumenty zawierające wyniki, opracowania, protokoły, notatki b) Segregator nadzoru pedagogicznego c) Segregator ewaluacji wewnętrznej
Zbiór 15: Notatki służbowe oraz postępowanie dyscyplinarne a) Skoroszyt notatek służbowych b) Skoroszyt upomnień i nagan
Zbiór 16: Ewidencja osób przystępujących do egzaminów zewnętrznych a) Segregator sprawdzianu zewnętrznego po klasie VI b) Zbiór elektroniczny na stronie OKE – serwis OBIEG c) Wydruki z systemów
Zbiór 17: Dokumentacja dotycząca awansu zawodowego a) Skoroszyty i teczki zawierające opinie dotyczące awansu zawodowego b) Skoroszyty wyróżnień, odznaczeń, nagród, wnioski o odznaczenia itp. c) Skoroszyty dotyczące awansu zawodowego d) Skoroszyty wniosków o nagrody
Zbiór 18: Księgi druków ścisłego zarachowania: a) Księga arkuszy ocen b) Księga świadectw c) Księga dzienników lekcyjnych d) Rejestr wydanych legitymacji e) Rejestr wydanych kart rowerowych

Zbiór 19: Zbiór upoważnień a) Segregator z upoważnieniami dyrektora szkoły b) Skoroszyt z rejestrem nazw użytkownika, loginów i haseł do komputerów, aplikacji, programów, poczty, w których są przetwarzane dane osobowe
Zbiór 20: Protokoły rad pedagogicznych, księga uchwał, księga zarządzeń: a) Księga zarządzeń b) Protokoły Rad Pedagogicznych c) Uchwały Rady Pedagogicznej
Zbiór 21: Akta osobowe pracowników
Zbiór 22: Karty zgłoszenia na konkursy międzyszkolne oraz zgody uczestników konkursów do przetwarzania wizerunku i danych osobowych a) Teczki zakładane przez osoby odpowiedzialne za organizację i przeprowadzenie konkursów
Zbiór 23: Umowy zawierane z osobami fizycznymi
Zbiór 24: CV i podania o przyjęcie do pracy
Zbiór 25: Dokumenty archiwalne: a) Archiwum dzienników lekcyjnych i pozalekcyjnych b) Archiwum dokumentacji dotyczących finansowania obiadów z MOPR c) Archiwum pism wychodzących i przychodzących d) Archiwum teczek wychowawców e) Archiwum dokumentacji konkursowych f) Archiwum obiadów
Zbiór 26: System EdPlan – ewidencja uczniów z orzeczeniami o potrzebie kształcenia specjalnego

Powyższy wykaz zbiorów ma charakter przykładowy i nie wyczerpuje wszystkich zbiorów danych osobowych w konkretnej placówce, nie stanowi również sztywnego wzoru do grupowania dokumentów. Każda placówka powinna dokonać własnej analizy tworzonych, przetwarzanych i przechowywanych danych i grupy zbiorów dostosować do swojej specyfiki.

Załącznik nr 3. Przykładowa zgoda na wyjazd na wycieczkę

Wyrażam zgodę na udział mojego syna/córki _____
/imię i nazwisko dziecka, klasa/
na wyjazd do _____, w celu wzięcia udziału w _____,
która odbędzie się _____/data/ r. w godz. _____
Wyjazd ze szkoły o godz. ____ powrót ok. godz. _____.
Transport /bus, autokar, pociąg…/ – _____.
Wycieczka jest organizowana przez _____
Jednocześnie oświadczam, że dziecko jest uczulone na leki/pokarmy:_____ .
Jeśli dziecko wymaga podania środka na chorobę lokomocyjną, zostanie w ten środek wyposażone w domu, a nauczyciel zostanie o tym poinformowany.
Jeśli dziecko pobiera na stałe leki, będzie w nie wyposażone, a nauczyciel zostanie o tym poinformowany.
W razie biegunki syn/córka może przyjąć preparat_____. /nazwa preparatu/
W razie potrzeby syn/córka może przyjąć środek przeciwbólowy_____. /nazwa leku/
Inne informacje: _____.
Telefon kontaktowy do rodziców (obowiązkowo)_____

Miejscowość, data _____

_____
/czytelny podpis rodzica/prawnego opiekuna/

Załącznik nr 4. Przykładowa zgoda na publikację zdjęć

Wyrażam zgodę/nie wyrażam zgody* na publikację przez Zespół Szkół nr 15 w Chełmie zdjęć oraz informacji o osiągnięciach mojego dziecka _____
/imię nazwisko dziecka, klasa/
ucznia Zespołu Szkół nr 15 w Chełmie, na stronie internetowej szkoły (www.szkolapietnastka.pl) oraz w mediach (prasa, internet, radio, TV) w celu informowania o sukcesach naukowych, sportowych i szkolnych. Administratorem przetwarzanych danych jest Zespół Szkół nr 15 w Chełmie, ul. Groszkowa 1, 22-100 Chełm.

Miejscowość, data _____

_____
/czytelny podpis rodzica/prawnego opiekuna/

* właściwe podkreślić

Załącznik nr 5. Przykładowa zgoda do konkursu międzyszkolnego

Informatyczny konkurs plastyczny *Szczepionka na wirusa*

Zgoda rodziców/opiekunów prawnych dziecka

OŚWIADCZENIE

Oświadczam, że wyrażam zgodę na opublikowanie na **stronie internetowej Szkoły Podstawowej nr 25 w Chełmie, Stowarzyszenia Przyjaciół Integracji oraz w mediach** imienia i nazwiska dziecka, zdjęcia z rozdania nagród i pracy plastycznej, nazwy szkoły, do której uczęszcza, i uzyskanych przez nie wyników w informatycznym konkursie plastycznym ***Szczepionka na wirusa***.

.....
/imię i nazwisko dziecka/

.....

.....
/nazwa szkoły/

.....
/data i czytelny podpis rodziców/

Załącznik nr 6. Przykładowa klauzula informacyjna

Zgodnie z art. 24 ust. 1 *Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* (Dz.U. 2002 nr 101, poz. 926, z późn. zm.) informuję, że administratorem Pani/Pana danych osobowych jest Szkoła Podstawowa nr 15 z siedzibą w Chełmie przy ul Groszkowej 1.

Pani/Pana dane osobowe będą przetwarzane w celu realizacji Programu X i nie będą udostępniane innym odbiorcom. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz ich poprawiania. Podanie danych osobowych jest dobrowolne.

Załącznik nr 7. Zgoda na przetwarzanie danych osobowych w procesie rekrutacji

Na podstawie art. 24 ust. 1 *Ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r.* (tekst jednolity: Dz.U. 2002 nr 101, poz. 926) wyrażam zgodę na gromadzenie i przetwarzanie danych osobowych moich i mojego dziecka. Dane osobowe będą przetwarzane w procesie rekrutacji na rok szkolny 2014/2015. Administratorem danych jest Szkoła Podstawowa nr 15 z siedzibą w Chełmie przy ul. Groszkowej 1.

_____

/data i czytelny podpis/

Załącznik nr 8. Scenariusz przykładowych zajęć dla rady pedagogicznej

Temat: Ochrona danych osobowych

Cele:

- Zapoznanie rady pedagogicznej z prawami i obowiązkami osób chroniących dane osobowe oraz osób, które te dane dotyczą.
- Zapoznanie rady pedagogicznej z polityką bezpieczeństwa danych osobowych w placówce oświatowej/szkole.
- Zapoznanie rady pedagogicznej z konsekwencjami nieprzestrzegania zapisów ustawy o ochronie danych osobowych.

Czas	**Przebieg**	**Materiały**
45 minut	Prowadzący zapoznaje członków rady pedagogicznej z przepisami prawnymi o ochronie danych osobowych: • *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* (Dz.U. 1997 nr 133 poz. 883), • *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. 2004 nr 100 poz. 1024).	Rzutnik, komputer, prezentacja

	Prowadzący w trakcie dyskusji z radą pedagogiczną pozyskuje informacje o: • danych osobowych gromadzonych na terenie szkoły, • o potrzebie i sposobach gromadzenia, ochrony, przechowywania danych osobowych na terenie danej placówki (w zależności od liczby osób, można wstępnie zaproponować dyskusję między nauczycielami w grupach). W trakcie dyskusji prowadzący porządkuje i uzupełnia informacje na temat zbiorów danych osobowych gromadzonych i przetwarzanych na terenie szkoły. Wprowadza podstawowe pojęcia, takie jak: dane osobowe, zbiór danych, przetwarzanie danych.	Tablica, duży arkusz do zapisywania informacji przez nauczycieli, kreda lub kolorowe markery Rzutnik, komputer, prezentacja z uporządkowanymi informacjami
60 minut	Prowadzący zapoznaje członków rady pedagogicznej z polityką bezpieczeństwa danych osobowych w szkole: • Wprowadza pojęcia: administrator danych, zgoda osoby, której dane dotyczą, system informatyczny, zabezpieczenie w systemie informatycznym, usuwanie danych, odbiorcy danych, administrator sieci, osoba upoważniona, poufność danych, identyfikator użytkownika, hasło, nośniki danych osobowych. • Zapoznaje z procedurami rozpoczęcia, zawieszenia i zakończenia pracy na komputerze. • Uczy, jak należy postępować z przedmiotami zawierającymi dane osobowe lub umożliwiającymi dostęp do nich. • Zapoznaje z konsekwencjami prawnymi naruszenia zapisów Ustawy.	Rzutnik, komputer, prezentacja