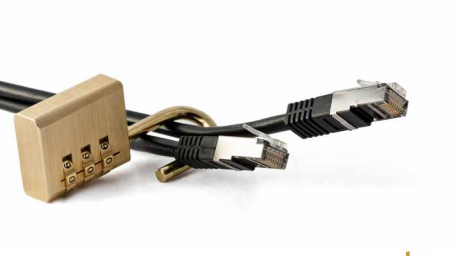

Podaj login i hasło

Przetwarzanie danych osobowych w systemach informatycznych w szkołach

W dzisiejszych czasach przetwarzanie danych, w tym również przetwarzanie danych osobowych, nie może się odbywać bez użycia systemów informatycznych.

Paradoksalnie rozważania na temat przetwarzania danych osobowych w systemach informatycznych należy rozpocząć od „rozebrania" na części pierwsze 2 podstawowych dokumentów wymaganych przez *Ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* (t.j. Dz.U. z 2002 r. Nr 101 poz. 926 ze zm., dalej: *Ustawa*), a ściślej rzecz biorąc przez *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. z 2004 r. Nr 100 poz. 1024, dalej: *Rozporządzenie*). Chodzi tu o Politykę bezpieczeństwa informacji oraz Instrukcję zarządzania systemem informatycznym, wykorzystywanym do przetwarzania danych osobowych.

Elementy funkcjonalne, narzucone aplikacjom wykorzystywanym do przetwarzania danych osobowych przez *Rozporządzenie*, są niezwykle istotne z punktu widzenia zabezpieczenia szkoły przed negatywnymi skutkami wizyty inspektorów GIODO.

POLITYKA BEZPIECZEŃSTWA INFORMACJI

Polityka bezpieczeństwa informacji jest dokumentem, na który składa się zestaw postanowień i wytycznych regulujących sposób zarządzania bezpieczeństwem informacji, w tym również danych osobowych administratora danych (warto przypomnieć, że jest to podmiot decydujący o celach i środkach przetwarzania danych – tu: szkoła reprezentowana przez dyrektora).

§ 4 *Rozporządzenia* wymaga, aby polityka bezpieczeństwa zawierała: „(…)

1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
4) sposób przepływu danych pomiędzy poszczególnymi systemami;
5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych".

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM WYKORZYSTYWANYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Zawartość merytoryczną Instrukcji reguluje § 5 *Rozporządzenia*, zgodnie z którym dokument ten powinien zawierać:

- procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności,
- stosowane metody i środki uwierzytelnienia oraz procedury związane z zarządzaniem nimi i ich użytkowaniem,
- procedury rozpoczęcia, zawieszenia i zakończenia pracy, przeznaczone dla użytkowników systemu,
- procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania,
- sposób, miejsce i okres przechowywania elektronicznych nośników informacji, zawierających dane osobowe oraz kopie zapasowe,
- sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania inwazyjnego,
- sposób odnotowania informacji o odbiorcach,
- procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Niestety nie jest to miejsce na szczegółowe omawianie wskazanych powyżej dokumentów, niemniej jednak są one na tyle istotne dla prawidłowości funkcjonowania pro-

cesów przetwarzania danych osobowych, że zupełne spuszczenie zasłony milczenia na te zagadnienia niewątpliwie zaowocowałoby pokaźną luką w wiedzy czytelnika na temat ochrony danych osobowych przetwarzanych w szkołach.

WYMAGANIA FUNKCJONALNE APLIKACJI

Każda aplikacja informatyczna wykorzystywana do przetwarzania danych osobowych musi, zgodnie z § 7 *Rozporządzenia*, umożliwiać odnotowanie:

a) daty pierwszego wprowadzenia danych konkretnej osoby – przy wprowadzaniu danych osoby X system informatyczny powinien odnotować datę wprowadzenia tych danych do bazy; ważne jest, aby modyfikacja danych nie powodowała zmiany daty, o której tu mowa,

b) identyfikatora użytkownika wprowadzającego dane – przy wprowadzaniu danych osoby X system informatyczny powinien odnotować login użytkownika wprowadzającego dane do bazy; ważne jest, aby modyfikacja danych nie powodowała zmiany odnotowanego loginu,

c) źródła danych, jeśli dane nie są zbierane od osoby, której dotyczą – jeśli dane osoby X pozyskujemy z innych źródeł niż osoba X, wówczas w systemie informatycznym musi pojawić się informacja, skąd zostały one pozyskane; warto zaznaczyć, że źródłem danych nie jest formularz internetowy, ale osoba wypełniająca ten formularz; dobrym przykładem systemu informatycznego, w którym zwykle nie jest konieczne odnotowanie źródła pozyskania danych, są aplikacje kadrowe,

d) informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia,

e) sprzeciwu wobec przetwarzania danych w celach marketingowych.

Należy pamiętać, że informacje wskazane w punktach a) i b) muszą zostać odnotowane przez system informatyczny automatycznie, co oznacza, że bezpośrednio po wprowadzeniu do bazy informacji o jakiejkolwiek osobie system informatyczny niejako samoczynnie odnotowuje, kto (odnotowując identyfikator/login) i kiedy (pobierając datę systemową) dokonał tej operacji. Istotne jest też, aby aplikacja umożliwiała sporządzenie oraz wydrukowanie raportu zawierającego wszystkie informacje wskazane w punktach od a) do e).

Wyszczególnione powyżej elementy funkcjonalne, narzucone aplikacjom wykorzystywanym do przetwarzania danych osobowych przez *Rozporządzenie*, są niezwykle istotne z punktu widzenia zabezpieczenia szkoły przed negatywnymi skutkami wizyty inspektorów GIODO. Każda kontrola GIODO sprawdza bowiem możliwość odnotowania wymaganych informacji we wszystkich systemach informatycznych wykorzystywanych do przetwarzania danych osobowych.

Wypada tu nadmienić, że kontrole przeprowadzone w szkołach przez GIODO w 2008 r. wykazały niezbicie, że systemy Hermes i SIO, które, jak wiemy, zostały narzucone szkołom przez jednostki nadrzędne, nie spełniały wskazanych powyżej wymagań funkcjonalnych *Rozporządzenia*. Problem ten został dostrzeżony przez GIODO, który zwrócił się do ministra edukacji narodowej z prośbą o podjęcie działań, mających na celu dostosowanie tych systemów informatycznych do wymogów wynikających z przepisów o ochronie danych osobowych. Stan ten – bądź co bądź niezgodny z prawem – nie uległ jednak zmianie od 2008 r.

USTAWOWE POZIOMY BEZPIECZEŃSTWA

Można przyjąć, że wymagania *Rozporządzenia* dotyczące zabezpieczenia przetwarzania danych osobowych nie są szczególnie wygórowane. *Rozporządzenie* nieco sztucznie wprowadza 3 poziomy bezpieczeństwa:

- **podstawowy** – stosujemy go, gdy w systemie informatycznym nie są przetwarzane tzw. dane wrażliwe (wymienione w art. 27 *Ustawy*) i nie ma on żadnego połączenia z internetem,

System informatyczny, w którym przetwarzane są dane osobowe, należy odpowiednio zabezpieczyć przed działaniami hakerskimi

Niezbędne jest przesyłanie wszelkich danych osobowych w postaci zabezpieczonej – szyfrowanej

- **podwyższony** – stosowany, gdy w systemie informatycznym przetwarzane są dane wrażliwe i żadne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych, nie jest połączone z internetem,
- **wysoki** – stosujemy go, gdy mamy dostęp do internetu, bez rozróżnienia kategorii danych przetwarzanych w zbiorach.

Na dobrą sprawę różnica pomiędzy poziomem podstawowym a podwyższonym w stosowanych zabezpieczeniach polega wyłącznie na stopniu skomplikowania hasła. Na poziomie podstawowym wystarczy stosować hasło 6-znakowe. Na poziomie podwyższonym hasło musi natomiast składać się z min. 8 znaków, zawierać co najmniej jedną wielką literę, cyfrę lub znak specjalny. W obu przypadkach hasło należy zmieniać nie rzadziej niż co 30 dni.

Niezbędnym elementem bezpiecznego przetwarzania danych osobowych jest również systematyczne tworzenie kopii bezpieczeństwa i przechowywanie ich poza miejscem produkcyjnego przetwarzania danych.

Skoro już wspomnieliśmy o hasłach, oczywiste jest, że systemy wykorzystywane do przetwarzania danych osobowych muszą być wyposażone w mechanizmy kontroli dostępu, czyli system logowania, który najczęściej ciągle jeszcze oparty jest na identyfikatorze użytkownika (tzw. loginie) oraz przyporządkowanym do niego haśle. Ważne jest, aby login należał wyłącznie do jednej, konkretnej osoby i nie był nigdy przyznawany innym użytkownikom.

Poziomy podstawowy i podwyższony wymagają również, co wydaje się oczywiste, „(…) stosowania zabezpieczeń przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego (…)", a więc instalacji oprogramowania antywirusowego. Pamiętać przy tym należy o bieżącym aktualizowaniu zarówno samego oprogramowania, jak i definicji wirusów. Stary „antywirus" z przestarzałymi definicjami jest bowiem równoznaczny z brakiem „antywirusa".

Kolejnym wymogiem jest zastosowanie urządzeń zabezpieczających system informatyczny przed utratą danych, spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej. Oznacza to, że komputery, na których przetwarzane są dane osobowe, niezależnie od tego, czy są serwerami, czy stacjami roboczymi, powinny zostać podłączone do sieci zasilającej poprzez urządzenia typu UPS (zasilacz awaryjny wyposażony najczęściej w akumulator; w przypadku przerwy lub zakłóceń dostawy energii elektrycznej z sieci energetycznej urządzenie przełącza się na pracę z akumulatora).

Niezbędnym elementem bezpiecznego przetwarzania danych osobowych jest również systematyczne tworzenie kopii bezpieczeństwa i przechowywanie ich poza miejscem produkcyjnego przetwarzania danych. Przechowywanie nośników zawierających kopie danych w serwerowni, gdzie odbywa się bieżące, produkcyjne procesowanie danych, z całą pewnością nie jest dobrym rozwiązaniem. Nośniki z danymi powinny być przechowywane w miejscach, do których dostęp mają wyłącznie osoby upoważnione. Co więcej, jeśli kopie przechowujemy np. w sejfie (bo jest bezpieczny), to zadbajmy też o to, żeby dostęp do niego posiadał niewielki krąg zaufanych ludzi, np. wyłącznie dyrektor.

W celu zminimalizowania ryzyka udostępnienia danych osobom nieupoważnionym kopie danych, zgodnie z *Rozporządzeniem*, należy usuwać trwale, bezpośrednio po ustaniu ich użyteczności. Istotną kwestią jest również konieczność usunięcia danych z nośników przeznaczonych do naprawy, likwidacji czy mających być przekazanych podmiotowi nieuprawnionemu do przetwarzania danych. Przez usunięcie danych rozumiemy postępowanie uniemożliwiające w jakikolwiek sposób odczytanie informacji. Zaznaczyć należy, że zwykłe systemowe „delete" nie spełnia tego warunku, ponieważ przy użyciu ogólnie dostępnych narzędzi możliwe jest odzyskanie i odczytanie usuniętych w ten sposób danych. Z trwale usuniętymi informacjami mamy do czynienia wtedy, gdy np. zostały one wielokrotnie nadpisane przy użyciu specjalistycznego oprogramowania lub kiedy ich nośnik został zniszczony fizycznie, w sposób uniemożliwiający jego reaktywację.

Kolejnym newralgicznym elementem przetwarzania danych osobowych są wszelkiego rodzaju urządzenia przenośne, takie jak np. notebook czy pendrive. W tym przypadku dobrze jest przyjąć jedyną słuszną, jednak – jak się okazuje w praktyce – nie dla wszystkich oczywistą zasadę: „Nie kopiujemy danych na przenośne urządzenia". Jeśli jednak, z jakichś bliżej nieokreślonych, ważnych lub bardzo ważnych powodów, absolutnie niezbędne jest przeniesienie danych na pendrive'a czy laptopa i wyniesienie ich poza bezpieczny obszar przetwarzania, to przepis mówi wyraźnie, że w takim przypadku konieczne jest zastosowanie środków ochrony kryptograficznej (np. szyfrowanie).

W ten oto płynny sposób przechodzimy do wymagań dla wysokiego poziomu bezpieczeństwa zdefiniowanego w *Rozporządzeniu*. Jak już wcześniej wspomniano, dotyczy on przetwarzania danych w systemach informatycznych połączonych w jakikolwiek sposób z internetem.

W dzisiejszych czasach stałe łącze jest raczej powszechnym zjawiskiem, a co za tym idzie, w większości przypadków administrator danych zwykle zobowiązany jest do stosowania zabezpieczeń na poziomie wysokim.

Zgodnie z *Rozporządzeniem* w tym przypadku system informatyczny służący do przetwarzania danych osobowych należy chronić przed zagrożeniami pochodzącymi z sieci publicznej (internetu) poprzez wdrożenie fizycznych lub logicznych zabezpieczeń, chroniących przed nieuprawnionym dostępem. Trudno zgadnąć, co autor przepisu miał na myśli, wskazując na zabezpieczenia fizyczne, bo przecież żadne sztaby nie ochronią systemu informatycznego przed działaniami hakerskimi, które mogą być prowadzone nawet z odległości tysięcy kilometrów. Prawdopodobnie chodzi o to, żeby odpowiednio zabezpieczyć obszar przetwarzania danych, w tym również pomieszczenia, gdzie zlokalizowany został sprzęt sieciowy, taki jak serwery czy routery.

Zabezpieczenia logiczne, o których mowa powyżej, obejmują działania mające na celu sprawowanie kontroli nad przepływem informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną oraz kontrolę nad działaniami inicjowanymi z sieci publicznej i sieci wewnętrznej szkoły. Mowa tu przede wszystkim o konieczności zastosowania odpowiednio skonfigurowanych urządzeń typu serwery proxy czy firewall. Jak najbardziej pożądanymi narzędziami zabezpieczającymi sieć wewnętrzną przed „inwazją" z zewnątrz są, obok firewalli, również systemy wykrywania i zapobiegania włamaniom typu IDS/IPS. Umożliwiają one zwiększenie poziomu bezpieczeństwa poprzez wzmocnienie kontroli komunikacji pomiędzy sieciami o różnym stopniu zaufania oraz implementację mechanizmów ostrzegania i blokowania ataków, wirusów oraz wszelkiego typu zagrożeń hybrydowych. Dokładnie rzecz biorąc, IDS służy do monitorowania oraz powiadamiania o zagrożeniach, a IPS dodatkowo podejmuje działania powstrzymujące ataki oraz minimalizuje ich skutki. IPS to obecnie chyba najbardziej skuteczny system zabezpieczenia sieci.

Poziom wysoki zabezpieczenia danych podejmuje też temat przesyłania danych przez internet. Co prawda w *Rozporządzeniu* jest mowa o konieczności szyfrowania danych służących wyłącznie do uwierzytelnienia, czyli np. identyfikatora użytkownika oraz odpowiadającego mu hasła, niemniej jednak pamiętać należy o art. 36 *Ustawy*, który streścić można następującymi słowami: administrator danych powinien zastosować środki bezpieczeństwa adekwatne do istniejących zagrożeń. W tym miejscu dochodzimy zatem do jedynego słusznego wniosku, że przesyłanie danych osobowych (nie tylko tych służących do uwierzytelnienia) przez internet w postaci jawnej z całą pewnością nie uwzględnia stosowania zabezpieczeń adekwatnych do zagrożeń. Z tego względu niezbędne jest przesyłanie wszelkich danych osobowych w postaci zabezpieczonej – szyfrowanej.

Na marginesie warto zaznaczyć, że konieczność stosowania środków bezpieczeństwa na poziomie wysokim nie zwalania administratora danych z obowiązku wykorzystania środków bezpieczeństwa wskazanych na poziomie podwyższonym i podstawowym.

Wymagania przywołanych tu aktów prawnych należy traktować wyłącznie jako niezbędne minimum. Zastosowanie narzucanych przez prawo rozwiązań w zakresie zabezpieczenia systemów informatycznych wykorzystywanych do przetwarzania danych osobowych chroni administratora danych, w tym wypadku szkołę (a co za tym idzie, jej dyrektora), wyłącznie przed konsekwencjami pokontrolnymi i to tylko do momentu, w którym nie okaże się, że jednak jakiś mniej lub bardziej zdolny uczeń pozyskał nieprzeznaczone dla niego dane i opublikował je na forum internetowym. W takim przypadku postępowanie prowadzone przez GIODO może prowadzić do jednego wniosku: „zastosowane zabezpieczenia nie są wystarczające". Uważny czytelnik zauważył pewnie, że podobne stwierdzenie stoi w jawnej opozycji do treści art. 36 *Ustawy*, o którym wspomniano kilka zdań wcześniej.

Systemy wykorzystywane do przetwarzania danych osobowych muszą być wyposażone w mechanizmy kontroli dostępu, czyli system logowania, który najczęściej oparty jest na identyfikatorze użytkownika (tzw. loginie) oraz przyporządkowanym do niego haśle.

W celu rzeczywistego zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe, należy zastosować nie tylko minimum wynikające z *Ustawy*, ale wszelkie dostępne w szkole środki i narzędzia, mogące wpłynąć na podniesienie poziomu bezpieczeństwa danych przetwarzanych w formie elektronicznej. Jak wynika z powyższych rozważań, pożądany stan osiągany jest poprzez analizę ryzyka, na podstawie której powstają procedury regulujące kwestie zarządzania bezpieczeństwem, tj. m.in. Polityka bezpieczeństwa oraz Instrukcja zarządzania systemem informatycznym. Kolejnym krokiem jest wybór aplikacji posiadających odpowiednie funkcjonalności, a następnie wdrożenie niezbędnych narzędzi systemowych i sprzętowych, zabezpieczających przetwarzane dane zarówno przed zagrożeniami wewnętrznymi, jak i zewnętrznymi.

Zdarza się oczywiście, że budżet szkoły nie nadąża za cenami ciągle unowocześnianych metod zabezpieczenia sieci. Problem ten jest zrozumiały, niemniej jednak bezpieczeństwa informacji, w tym danych osobowych (a w szczególności informacji przetwarzanych w szkole), nie należy spychać na koniec listy budżetowej. Wiele prawdy kryje się bowiem w stwierdzeniu: Chcesz spać spokojnie? Nie bądź minimalistą w obszarze bezpieczeństwa informacji.

Adam Myziak

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