

Bezpieczne przedszkole

Dane osobowe, administrator bezpieczeństwa informacji i systemy informatyczne



Tak jak przetwarzanie danych w dzisiejszych czasach nie może obejść się bez systemu informatycznego, tak administrator danych z prawdziwego zdarzenia nie może obejść się bez administratora bezpieczeństwa informacji.

ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

Administrator bezpieczeństwa informacji (ABI) jest osobą, która – jak sama nazwa wskazuje – jest odpowiedzialna za kreowanie i zarządzanie systemem bezpieczeństwa informacji w firmie czy instytucji. Wprowadzenie w Polsce *Ustawy o ochronie danych osobowych* (dalej: *Ustawa*) nałożyło na podmioty przetwarzające te dane obowiązek wyznaczenia administratora bezpieczeństwa informacji. Z czasem zrodziło to mylne przekonanie, że ABI w ramach swoich obowiązków może i powinien zajmować się wyłącznie ochroną danych osobowych. Oczywiście ten zakres pracy administratora bezpieczeństwa informacji jest również bardzo istotny. Nie wolno jednak zapominać, że właściwe zabezpieczenie danych osobowych jest ściśle powiązane z bezpieczeństwem innych informacji, takich jak np. dane finansowe czy biznesowe.

Bardzo często zdarza się, że funkcja ABI jest powierzana osobie odpowiedzialnej za kadry lub informatykowi. Z uwagi na fakt, iż ani w jednym, ani w drugim przypadku nie mamy do czynienia z osobą wyspecjalizowaną w zarządzaniu bezpieczeństwem informacji, rozwiązanie takie nie wydaje się być najwłaściwsze. ABI powinien dysponować dobrą orientacją w zakresie zagadnień prawnych związanych z przetwarzaniem danych, jak również technologii informatycznych, wykorzystywanych do przetwarzania danych.

ABI nie musi być pracownikiem etatowym. Możliwe jest skorzystanie z usług firmy zewnętrznej lub osoby zatrudnionej np. na podstawie umowy-zlecenia.

UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Każda osoba przed dopuszczeniem do przetwarzania danych osobowych musi otrzymać stosowne upoważnienie od administratora danych, czyli w tym przypadku dyrektora przedszkola. Wydanie upoważnienia należy poprzedzić odpowiednim przeszkoleniem takiej osoby w ramach obowiązujących w placówce przepisów oraz proce-

dur związanych z bezpieczeństwem danych osobowych. Po zapoznaniu się z wszelkimi niezbędnymi informacjami pracownik dopuszczony do przetwarzania danych osobowych powinien podpisać oświadczenie, w którym zobowiązuje się do przestrzegania obowiązujących przepisów zewnętrznych i wewnętrznych oraz do zachowania w tajemnicy wszelkich danych (z wyjątkiem tych jawnych), do których ma dostęp w ramach pełnionych przez siebie obowiązków służbowych.

Dopilnowanie właściwej realizacji wskazanych powyżej zadań spoczywa w całości na barkach administratora bezpieczeństwa informacji. Obowiązkiem ABI jest również prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych, zawierającej takie dane jak: imię i nazwisko, data nadania i ustania upoważnienia, zakres upoważnienia oraz identyfikator użytkownika w systemie informatycznym.

Warto pamiętać, aby bezpieczeństwa informacji, w tym szczególnie danych osobowych, nie spychać na koniec listy budżetowej.

SYSTEMY INFORMATYCZNE

Paradoksalnie rozważania na temat przetwarzania danych osobowych w systemach informatycznych należy rozpocząć od „rozebrania” na części pierwsze dwóch podstawowych dokumentów wymaganych przez *Ustawę*, a ściślej rzecz biorąc przez *Rozporządzenie MSWiA z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych* (dalej: *Rozporządzenie*). Chodzi tu o Politykę bezpieczeństwa informacji oraz Instrukcję zarządzania systemem informatycznym, wykorzystywanym do przetwarzania danych osobowych.

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. Zgodnie z wymaganiami *Rozporządzenia* Polityka bezpieczeństwa musi zawierać: „(...)

- 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”.

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

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM WYKORZYSTYWANYM DO PRZETWARZANIA DANYCH OSOBOWYCH

Zgodnie z prawem zawartość merytoryczna instrukcji powinna obejmować:

- ▶ 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 ich zarządzaniem i 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 kopii zapasowych,
- ▶ 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.

WYMAGANIA FUNKCYJNALNE 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 – jeżeli 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 być odnotowywane przez system informatyczny automatycznie, co oznacza, że bezpośrednio po wprowadzeniu do bazy informacji o osobie X system informatyczny niejako samoczynnie zapisuje, 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 przedszkola przed negatywnymi skutkami wizyty inspektorów GODO. Każda kontrola sprawdza bowiem możliwość odnotowania wymaganych informacji we wszystkich systemach informatycznych wykorzystywanych do przetwarzania danych osobowych.

USTAWOWE POZIOMY BEZPIECZEŃSTWA

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

- ▶ **podstawowy** – stosuje się go, gdy w systemie informatycznym nie są przetwarzane tzw. dane wrażliwe (wymienione w art. 27 *Ustawy*) i nie ma on żadnego połączenia z internetem,
- ▶ **podwyższony** – należy go stosować, gdy w systemie informatycznym przetwarzane są dane wrażliwe i żad-

ne z urządzeń systemu informatycznego, służącego do przetwarzania danych osobowych, nie jest połączone z internetem,

- **wysoki** – stosuje się 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 sześciocyfrowe. Na poziomie podwyższonym hasło musi natomiast składać się z min. ośmiu znaków, zawierać co najmniej jedną wielką literę, cyfrę lub znak specjalny. W obu przypadkach hasło należy zmieniać nie rzadziej niż co 30 dni.

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 hasłu. 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 antywirusowego, jak i definicji wirusów. Stary antywirus z przestarzałymi definicjami wirusów 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 za pomocą urządzenia typu UPS.

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.



Nie należy bagatelizować kwestii odpowiedniego zabezpieczenia danych osobowych

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.

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.

Każda osoba przed dopuszczeniem do przetwarzania danych osobowych musi otrzymać stosowne upoważnienie od administratora danych, czyli w tym przypadku dyrektora przedszkola.

Zgodnie z *Rozporządzeniem* 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. 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 przedszkola. 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 poprzez implementację mechanizmów ostrzegania i blokowania ataków, wirusów oraz wszelkiego typu zagrożeń hybrydowych.

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.

Wskazane powyżej wymagania należy traktować wyłącznie jako niezbędne minimum. Zastosowanie narzuconych przez prawo rozwiązań w zakresie zabezpieczenia systemów informatycznych wykorzystywanych do przetwarzania danych osobowych w niewielkim stopniu chroni administratora danych, w tym wypadku przedszkole (a co za tym idzie, jego dyrektora), wyłącznie przed konsekwencjami pokontrolnymi – i to też nie do końca.

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

Zdarza się oczywiście, że budżet przedszkola nie nadąża za cenami ciągle unowocześnianych metod zabezpieczenia sieci. Problem ten jest zrozumiały, niemniej jednak warto pamiętać, aby bezpieczeństwa informacji, w tym szczególnie danych osobowych, nie spychać na koniec listy budżetowej.

Podstawa prawna:

- *Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* (t.j. Dz.U. z 2002 r. Nr 101 poz. 926 ze zm.),
- *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).



Adam Myziak

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