



**BIURO
GENERALNEGO INSPEKTORA
OCHRONY DANYCH OSOBOWYCH**
Departament Orzecznictwa, Legislacji i Skarg

DOLiS – 035 – 2919/15/KK

Warszawa, dnia 18 lutego 2016 r.

**Pani
E.L.
Dyrektor Poradni Psychologiczno-
Pedagogicznej**

W związku z Pani pismem, które do Biura Generalnego Inspektora Ochrony Danych Osobowych wpłynęło w dniu (...) sierpnia 2015 r., uprzejmie dziękuję za zainteresowanie problematyką ochrony danych osobowych, która uregulowana jest przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2015 r., poz. 2135, z późn. zm., dalej: ustawa o ochronie danych osobowych, ustawa). Wiążące stanowisko Generalnego Inspektora w przedmiocie zbadania, czy dane osobowe są przetwarzane zgodnie z prawem – co do zasady – może być zawarte jedynie w treści decyzji administracyjnej po przeprowadzeniu postępowania administracyjnego, w toku którego zostaną ustalone wszystkie okoliczności sprawy mające istotne znaczenie dla jej rozstrzygnięcia, na podstawie stosownych przepisów prawa.

W odpowiedzi na Pani pytanie uprzejmie informuję, iż zgodnie z art. 36 ust. 1 ustawy, administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

W odniesieniu do zagrożeń związanych z wymianą informacji poprzez sieć publiczną, pkt. XII załącznika do 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. z 2004 r. Nr 100, poz. 1024), stanowi, że administrator danych powinien wdrożyć urządzenie lub rozwiązanie logiczne zapewniające odpowiedni poziom ochrony przed zagrożeniami pochodzącymi z sieci publicznej. Rozwiązania te powinny zapewnić kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną. Kontrola ta może być oparta na instalacji specjalistycznego oprogramowania, które analizuje i rejestruje przepływ informacji na styku lokalnej sieci administratora danych z siecią publiczną oraz podejmuje zaprogramowane decyzje np. w zakresie czy daną informację przekazać do sieci lokalnej czy też zablokować z uwagi na związane z nią zagrożenie. Oprogramowanie, o którym wspomniano wyżej, wykorzystywane do analizy tego ruchu to systemy antywirusowe, antyspamowe, firewalle, IDS-y, IPS-y i inne, które należy wdrożyć w odpowiednich miejscach w strukturze lokalnej sieci administratora danych. Systemy te mogą być instalowane jako oddzielne, niezależne programy lub jako elementy określonych pakietów sprzętowo – programowych stanowiących wielofunkcyjne zapory sieciowe zintegrowane w postaci jednego urządzenia UTM (ang. Unified Threat Management).

Urządzenia tego typu oferują różne funkcje, w tym głównie: filtra antyspamowego, filtra antywirusowego, sondy wykrywającej i blokującej próby włamań, filtra treści stron internetowych, routera, VPN, translatora adresów (NAT) i inne. Wśród tych innych funkcji systemu UTM mogą być np. kontrola aplikacji, kontrola sieci bezprzewodowej WiFi), czy ochrona przed wyciekiem danych (funkcja DLP). Wymienione rozwiązania, jeśli zostaną właściwie wdrożone i będą monitorowane, są w stanie wypełnić zobowiązanie administratora danych w zakresie zabezpieczenia systemu w sposób określony w punkcie XII.2 załącznika do wyżej wymienionego rozporządzenia.

Na zakończenie wskazuję, że więcej informacji na temat zasad przetwarzania danych osobowych, w tym treść obowiązujących we wspomnianej materii aktów prawnych, jak również wskazówki co do ich stosowania w praktyce można znaleźć na stronie internetowej Biura Generalnego Inspektora Ochrony Danych Osobowych, pod adresem: www.giodo.gov.pl, jak również na stronie internetowej <https://edugiodo.giodo.gov.pl>. **W szczególności polecam uwagę nowy serwis Generalnego Inspektora – ABI Informator – dostępny pod adresem www.abi.giodo.gov.pl.** Jest on dedykowany zagadnieniom związanym z powoływaniem, statusem oraz zadaniami jakie ciąży na Administratorze Bezpieczeństwa Informacji, który ma zapewniać przestrzeganie przepisów o ochronie danych osobowych.