

GDRP: za co odpowiada klient, a za co dostawca

25 maja 2018 roku wejdą w życie nowe przepisy dotyczące ochrony danych osobowych. Czasu na zmiany pozostało niewiele, a dostawcy rozwiązań i ich klienci nadal mają wiele wątpliwości, jaka będzie wykładnia prawa.

■ ARTUR PĘCZAK

Czy zaszyfrowane dane przestają być danymi osobowymi, czy dostawcy IT powinni dostosowywać oferowane przez siebie systemy w ramach umów utrzymaniowych, wreszcie czy prawo do zapomnienia oznacza konieczność usunięcia danych również z kopii zapasowych – nad tym między innymi zastanawiali się paneliści dyskutujący na poświęconej GDPR (RODO) debacie podczas premiery raportu „Computerworld TOP200”.

„GOTOWOŚĆ NA RODO”

W wielu ofertach sprzedażowych z zakresu bezpieczeństwa systemów oraz bezpieczeństwa danych pojawia się hasło „GDPRReady”, mające stanowić jasny przekaz dla klientów, że oferowane rozwiązania pomogą w spełnieniu wymagań wynikających z nowych uregulowań prawnych. „Co to znaczy: rozwiązanie gotowe na RODO? W mojej opinii jest to zestaw funkcjonalności, które prawidłowo zaimplementowane w organizacji pozwolą sprostać ustawie. Ale poza narzędziem potrzebna jest współpraca

między użytkownikami oraz określenie polityki organizacji w zakresie ochrony danych osobowych” – mówił Michał Baranowski z Proget. Wtórował mu Przemysław Mazurkiewicz z Commvault: „Z perspektywy dostawcy nie ma jednego narzędzia, które dotyczy wszystkich obszarów związanych z RODO. Wiele zależy od integratora, który powinien zaoferować klientowi spójne rozwiązanie dostosowane do wymagań prawnych konkretnej instytucji czy firmy. W pewnym sensie mowa jest więc tutaj o rozwiązaniach szytych na miarę danego klienta”.



Piotr Jabłoński z VMware zwrócił uwagę na inny aspekt tej sprawy: „Myślę, że na rynku nie ma rozwiązań, które byłyby dzisiaj zgodne z RODO. Jak można być zgodnym, skoro nie wiadomo jeszcze dokładnie, jaka będzie wykładnia prawa?”.

Operatorzy chmurowi zrzeszeni w ramach Cloud Infrastructure Service Provider in Europe (CISPE) deklarują dostarczanie usług zgodnie z zapisami rozporządzenia GDPR. Mamy tu jednak do czynienia jedynie z deklaracją zgodności, która nie jest weryfikowana przez żadne instancje nadrzędne czy kontrolne. Na tę kwestię zwrócił uwagę Piotr Jabłoński: „Ufamy, że tak jest, ale w umowie z dostawcą chmurowym musimy de facto mieć odrębne zapisy związane z ochroną danych osobowych. Deklaracja to jedno, drugie zaś to faktyczna egzekucja prawa”. Na rynku nie ma dzisiaj programu certyfikacji, który mógłby potwierdzić zgodność rozwiązania informatycznego z zapisami RODO. „Standard ISO 27018 dostosowywany jest pod kątem usług chmurowych, tutaj faktycznie można oczekiwać, że system ten będzie weryfikować takie rozwiązania pod kątem zgodności z regulacjami prawnymi. ISO 27018 będzie przyznawane i aktualizowane tylko dla rozwiązań, które spełnią tego typu wymagania” – wyjaśniał Piotr Jabłoński. Dla standardowych produktów i rozwiązań IT innych niż chmurowe takich certyfikacji nie razie nie ma.

WYKŁADNIA PRAWA

Dostawcy rozwiązań zwrócili uwagę na brak ostatecznych regulacji prawa oraz wykładni, która pomogłaby dostosować oferowane produkty do zapewnienia zgodności z RODO. „Technologia musi ustosunkować się do prawa, ale jak ma to zrobić, jeśli wykładnia prawa jest niejasna?” – zastanawiał się Piotr Jabłoński. Przemysław Mazurkiewicz z Commvault stwierdził, że liczy na opinie GIODO oraz wytyczne nadchodzące z Unii Europejskiej, które pomogą osiągnąć kompromis między uwarunkowaniami prawnymi a tym, co dzisiaj można osiągnąć przy użyciu technologii. „Cały czas czekamy na ostateczne wytyczne i sugestie, wykładnie i akty wykonawcze, które pomogą nam dostosować nasze produkty do obowiązującego prawa” – mówił Przemysław Mazurkiewicz.

Przedstawiciele administracji publicznej stwierdzili natomiast, że dostawcy nie powinni czekać na działania ustawodawców. „Podstawowe obowiązki w rozporządzeniu już są, a przepisy krajowe z perspektywy obowiązków, jakie ciążą na przedsiębiorcach, nie będą miały kluczowego znaczenia” – przekonuje Piotr Drobek, zastępca dyrektora Departamentu Edukacji Społecznej i Współpracy Międzynarodowej w Biurze GIODO. Wtórzy mu dr Maciej Kawecki z Ministerstwa Cyfryzacji, resortu projektującego przepisy o ochronie danych: „80% regulacji znajduje się w ogólnym rozporządzeniu, a krajowa ustawa o ochronie danych osobowych nie może w tym obszarze nakładać żadnych dodatkowych, rewolucyjnych obowiązków dla biznesu”. W pakiecie z ustawą instytucje będą zobowiązane do stosowania przepisów branżowych. „Rozluźnienie rygoru formy poprzez wprowadzenie zgody wyraźnej (ale nie pisemnej) otwiera drogę dla digitalizacji sektora ubezpieczeniowego w Polsce, który na tle innych krajów Unii w tym obszarze dopiero raczkuje” – wyjaśniał Maciej Kawecki.

PERSPEKTYWA UMÓW UTRZYMANIOWYCH

Dostawcy IT twierdzą, że teraz klienci nie wymagają, by w umowach wdrożeniowych czy utrzymaniowych zapewniona została zgodność rozwiązania z wymogami RODO. „Nie spotkaliśmy się z takimi żądaniami. Nasze umowy z klientami opierają się na ustandaryzowanych warunkach wsparcia. Zarówno w naszych umowach, jak i umowach innych dostawców zdefiniowana jest siła wyższa, do której zaliczamy również zmiany prawne” – mówił Przemysław Mazurkiewicz z Commvault. „Nie spotkaliśmy się z sytuacją, aby klienci wymagali od nas wprost spełnienia wymagań nadchodzących regulacji dotyczących ochrony danych. Mimo to wielu klientów pyta o te kwestie i ma świadomość, że już za chwilę trzeba być gotowym na nowe przepisy” – skomentował Michał Baranowski z Proget. Czy można żądać od dostawcy, aby już dzisiaj dostarczył nam system zgodny z RODO? Nie, bowiem obowiązek wykazania zgodności z Rozporządzeniem na nikim jeszcze nie ciąży. Ponadto w okresie przejściowym, a więc przez dwa lata od maja 2016 r., zarówno dostawcy, jak

i klienci mają czas, aby dostosować się do nowych regulacji. Sprawa okazuje się jednak bardziej skomplikowana, niż może się wydawać. Przykład stanowi umowa powierzenia danych osobowych. „Błędem popełnianym w umowach powierzenia danych może być wymóg spełnienia obowiązków, których jeszcze nie ma” – twierdzi Piotr Drobek z Biura GIODO. Zmian będzie wiele. Obecny administrator bezpieczeństwa informacji (ABI), a w przyszłości inspektor ochrony danych, będzie odgrywał dużo większą rolę w kontaktach ze światem zewnętrznym, niż dotychczas. W rezultacie umowa musi mapować takie zmiany jawnie określać, kiedy zostaną wdrożone i jak ten proces zmian zostanie przeprowadzony w praktyce.

SZYFROWANIE DANYCH

„Dane osobowe będą danymi nawet wtedy, gdy są zakodowane” – wyjaśniał Piotr Drobek. „Szyfrowanie jest jedną z metod zabezpieczenia danych.” Co więcej, RODO wprowadza nową kategorię danych osobowych, tzw. dane pseudonimowe. „Pojęcie to zostało wprowadzone, aby pokazać istnienie pewnych kategorii danych osobowych, które mają szczególny charakter, wynikający chociażby z tego, że zostały zaszyfrowane”.

ZAPOMNIENIE Z ZASTRZEŻENIAMI

Prawo do zapomnienia oznacza definitywne wykasowanie danych z nośników danych oraz kopii zapasowych. Dla dostawców systemów spełnienie tego wymagania może być trudne technologicznie. „Mimo skasowania danych z dysków magnetycznych bity informacji nadal pozostają na nich zapisane i można je odzyskać. Czy trzeba fizycznie skasować nośnik, aby uznać, że dane zostały usunięte? A może wystarczy nie używać dłużej tych danych, aby stwierdzić, że prawo do zapomnienia zostało zrealizowane?” – pytał Piotr Jabłoński z VMware. „W rozporządzeniu słowo: kopia zapasowa zostało wykorzystane literalnie” – poinformował dr Kawecki. Jeżeli dana osoba zażąda usunięcia swoich danych osobowych, stosowna operacja powinna obejmować również kopie zapasowe. „Dużą rolę odgrywa sposób zdefiniowania polityk kopii zapasowych oraz budo- wy archiwów. W tym obszarze na pewno uda się znaleźć rozwiązanie, w jaki ▶

W dyskusji dotyczącej GDPR podczas premiery raportu „Computerworld TOP200” udział wzięli sprawdzeni specjaliści z dziedziny ochrony danych osobowych, przedstawiciele administracji publicznej oraz dostawcy IT.

► **mec. Marcin Maruta** – partner w Kancelarii Radców Prawnych Maruta Wachta, moderator debaty

► **Piotr Drobek** – zastępca dyrektora Departamentu Edukacji Społecznej i Współpracy Międzynarodowej w Biurze GIODO

► **dr Maciej Kawecki** – zastępca dyrektora Departamentu Zarządzania Danymi w Ministerstwie Cyfryzacji

► **Michał Baranowski** – Product Manager w Proget

► **Piotr Jabłoński** – Senior Systems Engineer w VMware

► **Przemysław Mazurkiewicz** – dyrektor Działu System Engineering w Regionie EMEA East w Commvault

sposób zapewnić prawo do usunięcia danych osobowych. Przy dobrej analizie i klasyfikacji danych oraz zmianie procesów backupowych, np. w obszarze retencji danych, można co najmniej zbliżyć się do osiągnięcia tego celu” – stwierdził Przemysław Mazurkiewicz.

„Prawo do bycia zapomnianym więcej obiecuje, niż daje. Jeśli weźmiemy pod uwagę, kiedy to prawo może być zrealizowane, okazuje się, że 80% osób można spod tego prawa wyłączyć, bowiem istnieje jakaś inna przesłanka do przetwarzania danych osobowych, choćby prawnie uzasadniony interes. Jeśli jednak osoba będzie miała prawo żądać usunięcia danych, to wtedy z punktu widzenia GDPR powinno ono również obejmować usunięcie tych danych z kopii zapasowych” – dodał dr Maciej Kawecki. Wdrożenie mechanizmów trwałego (nieodwracalnego) usuwania wybranych danych z nośników pamięci i kopii zapasowych wymagać będzie zmian technologicznych oraz poniesienia istotnych kosztów na ich wdrożenie w środowisku produkcyjnym.

ŁAŃCUCH BŁOKÓW – BLOKADA ZAPOMNIENIA?

Blockchain na nowo definiuje sposób zawierania, rozliczania i zapisywania transakcji. Mechanizm ten ma zaimplementowanych kilka właściwości, w tym nieusuwalność i szyfrowanie danych, które wydają się trudne do pogodzenia z wymaganiami RODO. Czy z tej perspektywy technologia blockchain może być zgodna z RODO? Istota Blockchaina tkwi w niezaprzeczalności łańcucha transakcji. W momencie pozbawienia łańcucha choćby jednego ogniwa, przestaje on być łańcuchem i traci swoją podstawową właściwość, czyli niezaprzeczalność. To właśnie niezaprzeczalność wydaje się bardzo trudna do pogodzenia, np. z prawem do bycia zapomnianym, a więc prawem do żądania usunięcia swoich danych wynikającym bezpośrednio z RODO. „W działaniu każdej organizacji następuje etap, kiedy przestaje ona mieć podstawę prawną do przetwarzania danych osobowych. Każdy obywatel może bowiem zażądać usunięcia swoich danych, korzystając z prawa do bycia zapomnianym” – poinformował dr Maciej Kawecki z Ministerstwa Cyfryzacji.



Fot. PIOTR DZUBAK

„Szyfrowanie danych nie wyłącza stosowania przepisów o ochronie danych osobowych, co ma szczególne znaczenie, kiedy te dane transferowane są za granicę czy przetwarzane w ramach usług chmurowych”.

Piotr Drobek,
zastępca dyrektora
Departamentu
Edukacji Społecznej i Współpracy
Międzynarodowej
w Biurze GIODO

Problem w tym, że w przypadku łańcucha bloków będzie to trudne do zrealizowania. Sposobem obejścia problemu może być wyłączenie prawa do usunięcia danych osobowych w tym konkretnym przypadku. Dr Maciej Kawecki zwrócił uwagę na ważny aspekt tej sprawy: „Wyłączenie prawa do usunięcia danych pozbawi obywateli, czyli osoby, których te dane dotyczą, jednego z podstawowych praw wynikających z regulacji o ochronie danych osobowych. W Ministerstwie Cyfryzacji gromadzimy specjalistów od Blockchaina. Dyskutujemy i spieramy się, jak pogodzić tę technologię z ogólnym rozporządzeniem o ochronie danych osobowych. To także istotny temat dla Generalnego Inspektora Ochrony Danych Osobowych i Grupy Roboczej Artykułu 29”. Piotr Drobek z GIODO stwierdził, że w kontekście Blockchaina konieczne będzie zidentyfikowanie tych elementów, które mogą wywoływać wątpliwości lub być niezgodne z rozporządzeniem. Blockchain nie jest pierwszą technologią na rynku, która zauważalnie wpływa na prywatność i ochronę danych osobowych. Ważne jednak, aby na zjawisko to spojrzeć nie tyle na poziomie ogólnym, ile na płaszczyźnie jej zastosowań.

KLIENCI ZYSKAJĄ, DOSTAWCY ZAROBIAJĄ?

W ocenie firmy Microsoft koszt dostosowania wszystkich systemów do nadchodzących zmian w prawie o ochronie danych osobowych wyniesie 5 mld USD. W trakcie debaty dostawcy rozwiązań technologicznych okazali się zgodni co do tego, że nowe przepisy pozytywnie wpłyną na ich biznes, zaś klientom pozwolą przeprowadzić zmiany organizacyjne i dostosować systemy do aktualnych trendów. Przemysław Mazurkiewicz stwierdził, że duże instytucje finansowe już dzisiaj bliskie są osiągnięcia zgodności z nowymi przepisami, ponieważ od dłuższego czasu pracowały nad wprowadzeniem zmian na podstawie wytycznych poprzedniej dyrektywy. Według niego w temacie ochrony danych najczęściej do zrobienia mają małe firmy, i to jego zdaniem są bardzo perspektywiczni klienci. Z kolei Piotr Jabłoński z VMware szansę dla małych przedsiębiorców dostrzegł w chmurze publicznej. Firmy nadal pozostaną administratorami danych

osobowych, natomiast za platformę technologiczną odpowiedzialny będzie dostawca chmury. „To technologiczna szansa dla chmury publicznej, która może napędzić biznes w naszym regionie. Mówię tutaj nie tylko o globalnych dostawcach, ale również o wielu istniejących w Polsce centrach danych, które mogą lepiej dostosować się do lokalnych, czy też sektorowych uwarunkowań w obszarze ochrony danych” – dodał Piotr Jabłoński. Michał Baranowski z Proget zwrócił z kolei uwagę na kwestie bezpieczeństwa mobilnego. „W małych i średnich przedsiębiorstwach konieczność ochrony urządzeń mobilnych pozostaje niezauważana” – zaznaczył.

BEZPIECZNY OBYWATEL I KLIENT

Obowiązki wynikające z RODO dotkną wkrótce większość podmiotów gospodarczych bez względu na to, w jakim zakresie przetwarzają one dane osobowe. Nowe przepisy są jednak bardziej elastyczne i adekwatne do aktualnych zagrożeń aniżeli dotychczas obowiązujące regulacje. Wiąże się to z większą odpowiedzialnością dostawców, którzy będą mogli wspomagać się np. regulacjami branżowymi. Piotr Drobek z Biura GIODO zaznaczył, że oczekuje, iż dostawcy IT wykażą bardziej proaktywne podejście do sposobu implementacji wytycznych RODO w praktyce. „Małe i średnie podmioty nie zawsze mogą zapewnić sobie obsługę prawną, która wskaże im punkty, które należy zmienić. W tym przypadku standardy wyznaczają dostawcy rozwiązań. Dotyczy to zarówno dostawców globalnych i lokalnych” – stwierdził. Dr Maciej Kawecki z Ministerstwa Cyfryzacji przekonywał, że reforma ochrony danych jest wyzwaniem nie tylko dla przedsiębiorców, ale również dla ustawodawcy oraz administracji publicznej, która musi stworzyć odpowiednie przepisy prawne i wdrożyć je w życie. Dostrzegł ogromną rolę organu nadzorczego, który musi wspierać instytucje, edukować użytkowników, a w przyszłości sprawnie egzekwować założenia GDPR. „Wszyscy musimy zgodzić się co do tego, że wraz z wejściem rozporządzenia w życie statystyczny Europejczyk będzie mógł się poczuć bezpieczniej, jeśli chodzi o ochronę danych osobowych” – spuentował dyskusję Michał Baranowski. ■