Warszawa, 2.08.2023 r.

Omówienie wytycznych AEPD dotyczących walidacji systemów kryptograficznych do ochrony przetwarzania danych osobowych

W dobie cyfrowej, gdzie dane osobowe stają się coraz bardziej cenne, ochrona tych danych jest kluczowa. W tym kontekście, Agencja Ochrony Danych w Hiszpanii (AEPD) opracowała szereg wytycznych dotyczących walidacji systemów kryptograficznych, które mają na celu ochronę przetwarzania danych osobowych. Te wytyczne są nie tylko odpowiedzią na rosnące zagrożenia dla prywatności, ale także próbą zdefiniowania standardów, które pomogą organizacjom w zabezpieczaniu danych, którymi zarządzają.

Artykuł ten ma na celu omówienie tych wytycznych, zrozumienie ich znaczenia i zastosowania, a także pokazanie, jak mogą one wpłynąć na praktyki związane z ochroną danych. Przeanalizujemy kluczowe elementy tych wytycznych, zwracając szczególną uwagę na to, jak walidacja systemów kryptograficznych może pomóc w ochronie danych osobowych.

Kryptografia

Kryptografia to nauka analizowania i odszyfrowywania kodów, szyfrów i kryptogramów. Jest to także działanie polegające na pisaniu w kodzie lub szyfrze. Kryptografia jest kluczowym elementem w dziedzinach takich jak bezpieczeństwo komputerowe i sieciowe, gdzie jest wykorzystywana do zabezpieczania informacji.

Kryptografia ma wiele zastosowań, od ochrony danych przesyłanych przez Internet, po zabezpieczanie transakcji finansowych. Istnieją różne metody kryptograficzne, w tym szyfrowanie, które polega na przekształcaniu czytelnych informacji w dane, które nie mogą być odczytane bez odpowiedniego klucza, oraz deszyfrowanie, które jest procesem odwrotnym do szyfrowania.

Kryptografia jest również używana do tworzenia cyfrowych podpisów, które mogą być używane do weryfikacji tożsamości osoby lub systemu, oraz do tworzenia skrótów, które są unikalnymi "odciskami palców" dla danych i są często używane w kontekście bezpieczeństwa informacji.

W dzisiejszych czasach kryptografia jest niezbędna do ochrony prywatności i bezpieczeństwa w cyfrowym świecie. Bez niej, nasze dane osobowe, finansowe i inne ważne informacje, byłyby narażone na ryzyko kradzieży lub manipulacji.

Dane zabezpieczone

Zaszyfrowane informacje, choć mogą wydawać się nieczytelne dla niepowołanych oczu, nadal są uważane za dane osobowe. Szyfrowanie jest jednym z mechanizmów ochrony, które można zastosować podczas przetwarzania danych osobowych. Może służyć jako skuteczne narzędzie pseudonimizacji, które zastępuje identyfikowalne dane unikalnymi identyfikatorami.

Jednakże, ważne jest, aby zrozumieć, że samo szyfrowanie nie oznacza anonimizacji danych. Mimo że dane są zaszyfrowane, nadal zachowują swój pierwotny charakter jako dane osobowe. Innymi słowy, informacje, które zostały zaszyfrowane, nie są uważane za zanonimizowane.

Co więcej, nawet jeśli klucz deszyfrujący zostanie utracony lub usunięty, nie zmienia to faktu, że zaszyfrowane informacje są nadal danymi osobowymi. Klucz deszyfrujący jest tylko narzędziem do odczytania zaszyfrowanych danych, a jego brak nie zmienia ich natury.

Podsumowując, zaszyfrowane informacje, niezależnie od stanu klucza deszyfrującego, są nadal danymi osobowymi i powinny być traktowane z odpowiednią ostrożnością i ochroną, zgodnie z wytycznymi AEPD.

Wytyczne AEPD

Dokument zawiera wytyczne:

- dotyczące walidacji systemów kryptograficznych do ochrony przetwarzania danych osobowych. Ma na celu pomoc administratorom i podmiotom przetwarzającym w spełnianiu obowiązków wynikających z Ogólnego Rozporządzenia o Ochronie Danych (RODO).
- co do znaczenie kryptografii w ochronie danych osobowych. Wyjaśnia, że kryptografia jest podstawowym narzędziem zapewniającym poufność, integralność i dostępność danych.
- co do wyjaśnienia procesu walidacji systemów kryptograficznych. Obejmuje to identyfikację wymagań bezpieczeństwa systemu, dobór odpowiednich algorytmów i protokołów kryptograficznych oraz ocenę bezpieczeństwa systemu.
- dotyczące zarządzania kluczami kryptograficznymi. Omawia znaczenie zarządzania kluczami w utrzymaniu bezpieczeństwa systemu kryptograficznego i podaje rekomendacje dotyczące generowania, dystrybucji, przechowywania i niszczenia kluczy.

Co ciekawe, na końcu wytycznych odbywa się dyskusja na temat znaczenia przeprowadzania regularnych audytów i przeglądów systemów kryptograficznych. Wynika z niej, że walidacja systemu kryptograficznego nie jest jednorazowym wydarzeniem, ale ciągłym procesem, który wymaga regularnego monitorowania i aktualizacji.

Podsumowanie

Zgodnie z art. 32 ust. 1 lit. b) regulacji, systemy szyfrowania, jak każde inne zabezpieczenia, muszą być regularnie sprawdzane, oceniane i testowane pod kątem ich skuteczności w ochronie praw i wolności osób fizycznych. To jest obowiązek zarówno administratorów danych, jak i podmiotów przetwarzających dane. Inspektorzy ochrony danych lub doradcy ds. ochrony danych powinni być zaangażowani w proces doradztwa i nadzoru nad regularnym procesem weryfikacji i oceny systemów szyfrowania.

Szyfrowanie jest skomplikowanym procesem, który obejmuje wiele aspektów przetwarzania danych. Nie powinno być implementowane w sposób prosty lub powierzchowny. Naruszenie systemu szyfrowania podczas przetwarzania danych osobowych może prowadzić do poważnych zagrożeń dla praw i wolności osób, których dane dotyczą. Identyfikacja takich zagrożeń wymaga nie tylko określenia, jakie dane zostały naruszone, ale także oceny potencjalnego wpływu takiego naruszenia na osoby, których dane dotyczą, oraz na społeczeństwo jako całość. Siła i niezawodność systemu szyfrowania muszą być proporcjonalne do potencjalnego wpływu takiego naruszenia.

Administratorzy danych muszą pamiętać, że żaden system bezpieczeństwa nie jest nieomylny, dlatego nie powinni polegać wyłącznie na szyfrowaniu jako jedynym środku zarządzania ryzykiem naruszenia praw i wolności osób. Od samego początku procesu przetwarzania danych, administratorzy powinni uwzględniać różne środki ochrony prywatności, aby zminimalizować potencjalne skutki naruszenia ochrony danych osobowych. Takie środki mogą obejmować polityki ochrony danych, domyślne ustawienia prywatności, minimalizację danych, wczesną anonimizację, pseudonimizację, usuwanie danych, agregację, niski poziom szczegółowości, przejrzystość, itp. Ponadto, administratorzy powinni opracować i wdrożyć plany awaryjne i mechanizmy zarządzania naruszeniami danych osobowych.

Mateusz Jakubik, Oficer Bezpieczeństwa Informacji iSecure Sp. z o.o.