DESLOCK
ENCRYPTION BY

ESET

Rozporządzenie o Ochronie Danych Osobowych - RODO

(z ang. General Data Protection Regulation - GDPR)

PRZEWODNIK

ENJOY SAFER TECHNOLOGY™

General Data Protection Regulation (GDPR) czyli Rozporządzenie o Ochronie Danych Osobowych (RODO) zastępuje dyrektywę 95/46/WE Parlamentu Europejskiego i Rady WE z 1995r.

Cele Rozporządzenia to:
1) wzmocnienie i ujednolicenie praw dotyczących prywatności w sieci i ochrony danych osób fizycznych na terenie Unii Europejskiej
2) uproszczenie regulacji bezpieczeństwa dla firm i organizacji obsługujących mieszkańców UE

Wspólne Rozporządzenie zunifikuje i zastąpi 28 dotychczasowych regulacji poszczególnych państw członkowskich, które Dyrektywę z 1995r. wdrażały w różnym stopniu i na różne sposoby.
8 kwietnia 2016r. Rada UE przyjęła rozporządzenie RODO i powiązaną z nim Dyrektywę. 14 kwietnia 2016r. Rozporządzenie i Dyrektywa zostały przyjęte przez Parlament Europejski, a 4 maja 2016r. ich oficjalne teksty opublikowano w Dzienniku Urzędowym Unii Europejskiej.

Rozporządzenie zacznie obowiązywać od 25 maja 2018 roku.

CO SIĘ ZMIENIA?

Kluczowe zmiany w reformie obejmują[1]:

- Prawo do wiedzy o naruszeniu bezpieczeństwa danych. Firmy i organizacje muszą **1)** informować kompetentne organy publiczne zajmujące się ochroną danych osobowych o każdym przypadku naruszenia bezpieczeństwa danych w przypadku, gdy może ono narazić osobę, której dane zostały naruszone oraz **2)** informować o naruszeniu samych zainteresowanych tak, by mogli przedsięwziąć odpowiednie kroki bezpieczeństwa. W Polsce organem publicznym zajmującym się ochroną danych jest Generalny Inspektor Ochrony Danych Osobowych - GIODO.
- Silniejsze egzekwowanie zasad bezpieczeństwa. Organy ochrony danych będą mogły karać firmy nie stosujące przepisów UE grzywną w wysokości nawet do 4% ich rocznego globalnego obrotu. Kary administracyjne nie są obligatoryjne, a o ich nałożeniu ma każdorazowo decydować rozpatrzenie indywidualnego przypadku. Organ nakładający karę nie będzie badał winy ani jej stopnia, a jedynie fakt zaistnienia danego naruszenia przepisów o ochronie danych osobowych.
- Jedno europejskie prawo ochrony danych zastępuje 28 regulacji działających do tej pory w państwach członkowskich EU. Korzyści finansowe z unifikacji prawa dla firm operujących w UE szacowane są na około 2,3 mld € rocznie.
- 72 godziny - w takim czasie należy poinformować organ nadzorczy (GIODO) o wykryciu naruszenia bezpieczeństwa danych.
- Prawa UE muszą być stosowane przy **1)** przekazywaniu za granicę danych osobistych przez aktywne w UE firmy oferujące swoje produkty i usługi (w tym bezpłatne) obywatelom UE oraz **2)** gdy firmy te monitorują zachowania osób w UE.
- „Zasada prywatności w ustawieniach domyślnych" i „Zasada prywatności w fazie projektowania". Ich podstawowym celem jest „wbudowanie" zasad ochrony prywatności w każdy projekt zakładający przetwarzanie danych osobowych tak, by od samego początku jego istnienia ochrona prywatności stanowiła jego część składową.

Zwiększenie przez UE bezpieczeństwa danych obliguje firmy i organizacje do adekwatnej ochrony wrażliwych danych osobistych, zdefiniowanych jako:

"informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;"[2]

Tak szeroka definicja pozwala ująć nawet najprostsze informacje odnoszące się do konkretnej osoby nawet niebezpośrednio.

1 Skrót informacji prasowej:
http://www.europarl.europa.eu/news/pl/news-room/20160407IPR21776/ochrona-danych-parlament-przyj%C4%85%C5%82-nowe-przepisy-przystosowane-do-ery-cyfrowej

2 http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016R0679&from=PL

OCHRONA DANYCH

Art. 32. RODO[3] poświęcony bezpieczeństwu przetwarzania danych stwierdza:

> *1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:*
>
> *a) pseudonimizację i szyfrowanie danych osobowych;*
>
> *b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;*
>
> *c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;*
>
> *d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.*

Szyfrowanie jest najprostszą i najbezpieczniejszą metodą ochrony danych spełniającą wymogi Artykułu 32. RODO i ustalonym środkiem ochrony danych. RODO zawiera też wytyczne dla efektywnego działania strategii disaster recovery, odzyskiwania haseł i systemów zarządzania kluczami dostępu.

Artykuł 30. RODO[3] wymaga, by rejestr czynności przetwarzania danych osobowych był prowadzony z uwzględnieniem technicznych i organizacyjnych wymogów bezpieczeństwa opisanych w Artykule 32. Oznacza to, że firmy i organizacje muszą być w stanie udowodnić, że ich dane i systemy są bezpieczne, a zaszyfrowane dane możliwe do odzyskania po awarii technicznej.

3 http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016R0679&from=PL

POWIADOMIENIA O NARUSZENIACH BEZPIECZEŃSTWA

Artykuł 33. RODO[3] wymaga powiadamiania organu nadzorczego o każdym przypadku naruszenia bezpieczeństwa danych osobowych. W razie takiego naruszenia organ ten musi zostać powiadomiony najpóźniej w ciągu 72 godzin od wykrycia naruszenia. Po upływie tego czasu każde powiadomienie będzie należało opatrzyć wyjaśnieniem, dlaczego dokument wpływa po terminie przewidzianym w Rozporządzeniu.

Artykuł 34. RODO[3] zawiera zalecenia dot. zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych:

> *1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu*

Jednakże dalej ten sam artykuł stwierdza:

> *3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:*
>
> *a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;*
>
> *b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;*
>
> *c) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.*

Badania wykazały, że im wcześniej powiadamia się o naruszeniu bezpieczeństwa danych, tym dotkliwsze są konsekwencje dla firmy, która do takiego naruszenia dopuściła. W tym przypadku szyfrowanie uważane jest za wystarczający środek uniemożliwiający naruszenie bezpieczeństwa i pozwalający chronić reputację firm, które naruszenia doświadczyły.

KARY

Do tej pory w przypadku naruszenia bezpieczeństwa danych winowajca miał czas na uszczelnienie luk w ich ochronie. Przekroczenie wyznaczonego terminu lub niedopełnienie wymogów prawnych skutkowało **karą administracyjną**. Po wejściu RODO kara administracyjna będzie mogła być wymierzana z automatu bez możliwości odwołania się.

Sam system kar został znacząco rozbudowany, a ich wysokość znacznie wzrosła. Wedle Artykułu 83. - Ogólne warunki nakładania administracyjnych kar pieniężnych - punkt 44 w zależności od skali zaniedbania może wynieść odpowiednio do **10 000 000 EUR** lub 2% całkowitego rocznego światowego obrotu z poprzedniego roku (decyduje wartość wyższa) i do **20 000 000 EUR** lub 4% całkowitego rocznego światowego obrotu z poprzedniego roku.

> ***Przykłady zaniedbań podlegających grzywnie:***
>
> - *Jeśli Administrator Danych Osobowych (ADO) nie wdrożył odpowiednich środków technicznych i organizacyjnych mających na celu ochronę praw osób, których dane dotyczą,*
> - *Jeśli ADO nie uwzględnił ochrony danych w fazie projektowania (na etapie projektowania systemu informatycznego),*
> - *Jeśli ADO nie zgłosił incydentu w ciągu 72h po stwierdzeniu naruszenia, organowi nadzorczemu (jeśli incydent skutkował naruszeniem praw lub wolności osób fizycznych).*
>
> *Z kolei Artykuł 5. - Zasady dotyczące przetwarzania danych osobowych - stwierdza:*
>
> *1. Dane osobowe muszą być:*
>
> *f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").*

Państwa członkowskie EU mają czas na wdrożenie regulacji RODO do maja 2018. Niektóre kraje UE już rozpoczęły prace nad dostosowaniem swoich przepisów do Rozporządzenia. W maju 2015r. holenderski senat zatwierdził projekt korygujący ustawę o ochronie danych osobowych pod kątem RODO. Tym samym Holandia opuściła grupę państw z najsłabszymi systemami prawnej ochrony danych stając się obecnie jednym z europejskich liderów bezpieczeństwa danych.

ROZWIĄZANIE: SZYFROWANIE

RODO wymaga od wszystkich firm i organizacji wdrożenia nowych procesów i polityk dających osobom większą kontrolę nad swoimi danymi osobowymi. Wymusi to powstanie nowych procesów i instrukcji, ponownego przeszkolenia osób uprawnionych do przetwarzania danych osobowych i dostosowania obecnych systemów do nowych realiów prawnych.

Kluczowe będzie też wdrożenie nowych praktyk bezpieczeństwa ze szczególnym naciskiem na szyfrowanie przetwarzanych danych, bo jedną z kluczowych wytycznych RODO jest zapewnienie odpowiedniego bezpieczeństwa danych osobowych, a według artykułu 32. ("Bezpieczeństwo przetwarzania") szyfrowanie jest właściwym do tego środkiem.

Wdrożenie szyfrowania prócz spełnienia wymogów RODO przyniesie Administratorom Danych Osobowych (ADO) również wymierne korzyści biznesowe - utrata urządzenia (np. laptopa czy pamięci flash) zawierającego dane osobowe nie będzie musiała prowadzić do kary, jeśli tylko zostało ono wcześniej zaszyfrowane sprawdzonym rozwiązaniem bezpieczeństwa.

Takim rozwiązaniem jest oprogramowanie DESlock+, które od lat pomaga firmom każdej wielkości szyfrować laptopy, nośniki wymienne i pliki. Produkty DESlock+ chronią wszystkie wersje systemu Windows od XP do Windows 10 szyfrowaniem zgodnym ze standardem FIPS 140-2, a ich system zarządzania kluczami i unikalny serwer zarządzający są przedmiotami zarejestrowanych patentów.

4 http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016R0679&from=PL

DESlock Encryption od ESET to rozwiązanie zaprojektowane z myślą o spełnieniu wymogów RODO w prosty i efektywny sposób.

Cel	DESlock Encryption od ESET
Ochrona danych w ramach organizacji	DESlock Encryption oferuje szyfrowanie plików, folderów i nośników wymiennych (USB) jako standardową funkcję ochrony danych na stacji roboczej.
Ochrona danych podczas transportu	DESlock+ Pro umożliwia szyfrowanie całej powierzchni dysku, nośników wymiennych i optycznych w celu ochrony danych podczas ich przenoszenia.
Ochrona danych a telepraca	W ramach 1 komercyjnej licencji DESlock Encryption użytkownik może zaszyfrować wszystkie swoje komputery z systemem Windows. Dodatkowo aplikacja DESlock+ Go pozwala również na odszyfrowanie i zaszyfrowanie plików na komputerze bez zainstalowanego rozwiązania DESlock+.
Ochrona przesyłu danych między lokalizacjami	Wszystkie wersje DESlock Encryption posiadają wtyczkę do klienta poczty MS Outlook, opcję szyfrowania zawartości schowka systemowego (umożliwiając przesyłanie zaszyfrowanych wiadomości dowolnym klientem poczty z poziomu przeglądarki www) i szyfrowania załączników. Szyfrowanie nośników optycznych pozwala na bezpieczny transport danych na dyskach CD i DVD.
Blokowanie / ograniczony dostęp do wybranych danych	Unikalna, opatentowana technologia współ--dzielenia kluczy szyfrujących ułatwia wdrażanie i zarządzanie rozbudowanymi środowiskami.
Dostęp do chronionych danych na żądanie	DESlock+ Enterprise Server umożliwia zdalne zarządzanie użytkownikami oraz prawami dostępu przy użyciu bezpiecznego łącza. Klucze mogą być przyznawane centralnie, a w razie potrzeby błyskawicznie odwoływane.
Bezpieczeństwo danych osobowych	DESlock Encryption wykorzystuje zaufane i potwierdzone algorytmy oraz metody szyfrowania zgodne ze standardem FIPS-140-2.
Bezpieczne usuwanie danych	Narzędzie DESlock+ Desktop Shredder bezpiecznie niszczy dane standardem DoD-5220.22-M, dzięki czemu ich odzyskanie jest już niemożliwe.

Dlaczego warto wybrać DESlock+?

1) Rozwiązanie jest transparentne dla użytkowników, oferując bardzo wysoki poziom bezpieczeństwa przy utrzymaniu prostoty korzystania jak z niezaszyfrowanych danych
2) Wygodne centralne zarządzanie z konsoli administratora: wdrażanie rozwiązania, szyfrowanie wszystkich komputerów i zarządzanie całym środowiskiem z jednego miejsca.
3) Użytkownicy mogą pracować na komputerach poddawanych szyfrowaniu bez żadnego spadku wydajności.
4) W przypadku kontroli spowodowanej np. utratą komputera rozwiązanie oferuje możliwość udowodnienia, że utracone urządzenie rzeczywiście było zaszyfrowane.
5) Możliwość zdalnego odzyskania hasła, gdy użytkownik zapomni go np. przebywając w delegacji.
6) Pełne wsparcie techniczne w języku polskim.

A co jeszcze?
Zapytaj swojego lokalnego dostawcę rozwiązań ESET!