GDPR

Co należy wiedzieć o GDPR?

Rozporządzenie zacznie obowiązywać 25 maja 2018 roku.

8 kwietnia 2016 r. Rada UE przyjęła rozporządzenie General Data Protection Regulation (GDPR) czyli Rozporządzenie o Ochronie Danych Osobowych (RODO) i powiązaną z nim Dyrektywę. 14 kwietnia 2016 r. Rozporządzenie i Dyrektywa zostały przyjęte przez Parlament Europejski.

Rozporządzenie ma na celu:
1) wzmocnienie i ujednolicenie praw dotyczących prywatności w sieci i ochrony danych osób fizycznych na terenie Unii Europejskiej (wspólne rozporządzenie zunifikuje i zastąpi 28 dotychczasowych regulacji poszczególnych państw członkowskich);

2) uproszczenie regulacji bezpieczeństwa dla firm i organizacji obsługujących mieszkańców UE.

Co to są dane osobowe (osobiste) chronione przez GDPR?

To „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" (http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016R0679&from=PL)

Co się zmienia?

- **Prawo do wiedzy o naruszeniu bezpieczeństwa danych**

– Firmy i organizacje muszą 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
– Firmy i organizacje muszą 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.

- **72 godziny** – w takim czasie należy poinformować organ nadzorczy (GIODO) o wykryciu naruszenia bezpieczeństwa danych.

- **„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.

• **Prawa UE muszą być stosowane**
– przy przekazywaniu za granicę danych osobowych przez aktywne w UE firmy oferujące swoje produkty i usługi (w tym bezpłatne) obywatelom UE
– gdy firmy te monitorują zachowania osób w UE.

Ochrona danych wg GDPR

Art. 32. RODO 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.

Wedle Artykułu 83. - Ogólne warunki nakładania administracyjnych kar pieniężnych - punkt 44 w zależności od skali zaniedbania kara za niedopełnienie wymogów prawnych 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 podlegające grzywnie

Artykuł 83 stwierdza, że podlega grzywnie:

a) Jeśli Administrator Danych Osobowych (ADO) nie wdrożył odpowiednich środków technicznych i organizacyjnych mających na celu ochronę praw osób, których dane dotyczą,

b)Jeśli ADO nie uwzględnił ochrony danych w fazie projektowania (na etapie projektowania systemu informatycznego),

c) Jeśli ADO nie zgłosił incydentu w ciągu 72h po stwierdzeniu naruszenia, organowi nadzorczemu (jeśli incydent skutkował naruszeniem praw lub wolności osób fizycznych).

Zgodnie z rozporządzeniem GDPR osoby zajmujące się kontrolą i przetwarzaniem danych powinny wdrażać najnowocześniejsze zabezpieczenia stosownie do zagrożeń i charakteru danych osobowych, które mają być chronione. Okazuje się jednak, że organizacje nie zawsze potrafią jednoznacznie wskazać, co dokładnie kryje się pod hasłem „najnowocześniejsze".

Przygotowanie polskich firm - GDPR

Wnioski płynące z: Badania ARC Rynek i Opinia, zorganizowanego przy współpracy z Trend Micro oraz VMware jesienią 2016 roku.

ZNAJOMOŚĆ GDPR:

1	Znajomość rozporządzenia GDPR wśród ogółu respondentów jest niepokojąco niska — **ponad połowa badanych (52%) do tej pory nie słyszała o reformie ochrony danych osobowych** (badanie było przeprowadzone we 9/10. 2016)
2	**Najniższa znajomość nowego prawa charakteryzuje sektor handlowy,** w którym aż 62% firm nie słyszało o wydanym przez Komisję Europejską rozporządzeniu.
3	**Znajomość GDPR jest najwyższa wśród pracowników sektora usług (56%).**

G

D

P

R

4 **Niespełna dwie trzecie badanych (61%) stwierdziło, że rozporządzenie GDPR będzie miało zastosowanie w przypadku ich firmy**, zaś prawie jedna piąta (18%) jest przeciwnego zdania; podobny odsetek (21%) nie ma sprecyzowanego poglądu na ten temat.

ODPOWIEDZIALNOŚĆ:

1 **67% uważa, że odpowiedzialność za stosowanie się do rozporządzenia GDPR ponosi cała organizacja,** a 31% sądzi, że jest nią obarczony dyrektor generalny (CEO) lub zarząd firmy.

2 **57% respondentów nie odnotowało faktu zaangażowania zarządu firmy w przygotowania do wdrożenia GDPR**. Mimo grożących kar finansowych i ogromnego ryzyka dla funkcjonowania firmy, brak świadomości sprawia, że osoby zarządzające nie angażują się póki co w przygotowania do wdrożenia nowego rozporządzenia.

3 Prawie żadna (96%) z przebadanych firm nie potrafiła wskazać, kto ponosi odpowiedzialność za naruszenie danych z Unii Europejskiej przetwarzanych przez usługodawcę spoza Unii Europejskiej np. z USA.

WYBÓR ROZWIĄZAŃ OCHRONY:

1. **Prawie jedna piąta firm (19%) nie wie, czym są najnowocześniejsze zabezpieczenia.** 50% badanych uważa, że są to rozwiązania oferowane przez doświadczonych liderów na rynku.

2. Aż 22% respondentów wskazało, że koszt jest silniejszym czynnikiem korzystania z poszczególnych zabezpieczeń niż zapewnienie „najnowocześniejszej" ochrony.

G

D

P

R

3. **17% firm uważa, że decyzje o wdrożeniu konkretnych systemów zabezpieczających powinny być podejmowane na podstawie raportów niezależnych analityków** z takich instytucji jak Gartner, Forrester, IDC etc.

PROBLEMY Z PRZESTRZEGANIEM PRZEPISÓW O OCHRONIE DANYCH:

1	Dla 24% badanych problemem jest brak formalnych procedur powiadamiania o naruszeniu (24%) oraz ograniczenia wynikające ze stosowanych systemów IT (20%)
2	Dla 19% to ograniczone zasoby na poprawę aktualnych procedur
3	Brak dostatecznej ochrony systemów informatycznych 17%
4	Brak formalnych procedur umożliwiających jednoznaczną identyfikację lokalizacji i właściciela danych 16%
5	Brak środków finansowych 15%
6	Brak jednoznaczności co do tego, kto odpowiada za ten obszar 15%
7	Brak skutecznej ochrony danych 15%

KROKI PODEJMOWANE W CELU ZWIĘKSZENIA BEZPIECZEŃSTWA:

1	Wdrożenie nowych rozwiązań, mających na celu usprawnienie obowiązujących systemów i procedur (16%). Kluczowymi inicjatywami w tym zakresie jest **stosowanie szyfrowania (81%) oraz zwiększenie świadomości pracowników w zakresie ochrony danych (80%).**

G

D

P

R

2 **Blokada sprzętu w celu uniknięcia użycia zainfekowanych nośników USB (66%)**

3 Wprowadzenie przejrzystych **procesów, które pozwalają na identyfikację, lokalizację oraz zabezpieczenie danych (65%)**

4 Wprowadzenie **technologii ochrony przed wyciekami (utratą) danych (57%)**

UŻYTKOWNICY WEWNĘTRZNI POWINNI ZASTANOWIĆ SIĘ NAD ZASTOSOWANIEM:

- **mechanizmów ochrony danych (takich jak szyfrowanie)**, dzięki którym dane osobowe są bezpieczne nawet w przypadku utraty urządzenia, w którym są przechowywane;
- **funkcji zdalnego wymazywania danych z urządzeń przenośnych**;
- **technologii zapobiegania utracie danych, które pozwalają kontrolować, jakiego rodzaju informacje są przesyłane w obrębie przedsiębiorstwa i poza nim.**

DODATKOWE MECHANIZMY KONTROLI UŻYTKOWNIKÓW ZEWNĘTRZNYCH:

- **blokady uniemożliwiające uruchamianie szkodliwego oprogramowania w punktach końcowych** (zarówno narzędzia chroniące przed szkodliwym oprogramowaniem, jak i technologie kontroli aplikacji w punktach końcowych);
- **szyfrowanie danych w urządzeniach przenośnych używanych poza siedzibą przedsiębiorstwa**;

G

D

P

R

- **poprawki wirtualne pozwalające zapobiec wykorzystaniu przez zdalnych użytkowników niezałatanych luk w zabezpieczeniach** (a tym samym ograniczyć ryzyko związane z korzystaniem z systemów operacyjnych i aplikacji, w których nie zainstalowano wymaganych poprawek);

- **rozwiązania do wykrywania włamań, które pozwalają wykryć naruszenie bezpieczeństwa sieci i podjąć właściwe działania, aby uniemożliwić osobom z zewnątrz kradzież cennych danych osobowych.**

Zalecenia dla firm i organizacji:

1. Zrozum/ustal, jakie dane są Ci potrzebne i jakie dane zbierasz. Ile danych przetwarzasz i czy potrzebujesz je zbierać lub przechowywać. Miej dostęp do mechanizmów, które pozwolą Ci bezpiecznie usunąć bezużyteczne dane.

2. Zidentyfikuj przepływ danych osobowych w organizacji/firmie i to, jak są przetwarzane, zabezpieczone, przechowywane i usuwane.

3. Oceń czy obecny poziom bezpieczeństwa jest wystarczający, aby zapewnić ochronę przed nieuprawnionym przetwarzaniem i utratą danych.

4. Przejrzyj wszystkie powiadamiania o naruszeniu, aby ocenić, czy firma posiada odpowiednie narzędzia, aby podjąć odpowiednie działania, czyli zgłosić incydent – w nieprzekraczalnym terminie 72 godzin.

G

D

P

R

PRZYGOTOWANIE

- **Data Loss Prevention (DLP)**

Ochrona przed wyciekiem danych. Usługa mająca za zadanie zapobiegać przed wyciekiem niepowołanych czy też wrażliwych danych – z naszej firmy do sieci zewnętrznej.

- **Privileged Acces Management (PAM)**

ograniczenia dostępu do danych. Tutaj pomóc mogą rozwiązania typu Privileged Acces Management (PAM). PAM to narzędzie do monitorowania uprzywilejowanych użytkowników, które: zarządza dostępem do kont uprzywilejowanych; daje możliwość śledzenia i wykrywania aktywności przy dostępie konsultantów i wsparcia z firm zewnętrznych; daje możliwość zarządzania hasłami; posiada możliwość nagrywania sesji; umożliwia śledzenie, audyt i potwierdzenie spełnienia zgodności z regulacjami i wymogami prawnymi.

OCHRONA I WYKRYWANIE

- **Advanced Threat Protection (ATP)**

Serwis zabezpieczający naszą sieć przed nieznanymi atakami ransomware, atakami typu **Zero-day** oraz zaawanasowanymi malwarami, na które nie ma sygnatur. Zagrożenia najczęściej działają długofalowo, pozostając niewykryte w sieci Klienta wyciągają informację bądź czekają uśpione do czasu osiągnięcia odpowiedniego poziomu „zarażenia” sieci. Zagrożenia tego typu są praktycznie niewykrywalne standardowymi metodami.

- **Szyfrowanie**

Ochrona wrażliwych danych. Możliwość szyfrowania całych powierzchni dysków, nośników wymiennych, pojedynczych plików oraz wiadomości e-mail. Mamy pewność, że dane zawarte na firmowych komputerach i osobistych urządzeniach mobilnych pracowników są chronione przed niepowołanym dostępem.

G

D

P

R

W przypadku przesyłania szczególnie wrażliwych danych można utworzyć zaszyfrowaną wiadomość, którą odczyta jedynie jej odbiorca posiadający ustalony klucz.

REAKCJA

- **Incident Response Plan (IRP) to inaczej plan zarządzania kryzysowego,** który pozwoli na podjęcie odpowiednich działań, czyli zgłoszenie incydentu w nieprzekraczalnym terminie 72 godzin.

Podsumowując:

GDPR stworzy dodatkowe obowiązki dotyczące bezpieczeństwa i prywatności, które firmy i organizacje będą musiały spełnić. Kierownictwo nie powinno czekać na wymuszanie na sobie ich zastosowania, zamiast tego dobrze byłoby zastanowić się, jak przygotować swoich pracowników, procesy i technologie by zapewnić firmie zgodność z wymogami, obowiązującymi od połowy 2018 roku.