




Biuletyn Bezpieczeństwa Komputerowego


RODO (GDPR)


Zarys Ogólny


Być może słyszałeś już o Rozporządzeniu UE o Ochronie Danych Osobowych (RODO/GDPR), które zacznie obowiązywać 25 Maja 2018 roku. RODO/GDPR obowiązywać będzie każdą organizację (niezależnie od jej lokalizacji na świecie), która przetwarza dane osobowe obywateli Unii Europejskiej. W celu zapewnienia zgodności z przepisami rozporządzenia, warto poznać i stosować kilka kluczowych zasad.

Każda osoba posiada prawo do prywatności. Organizacje powinny tą prywatność respektować, ograniczając zakres zbieranych i przetwarzanych danych osobowych, jak również dbając o ich właściwe zabezpieczenie. Zobowiązania dotyczące ochrony danych mają zastosowanie wobec każdej informacji (samej w sobie, lub wykorzystywanej z innymi fragmentami informacji), pozwalającej zidentyfikować indywidualnego obywatela Unii Europejskiej. Mogą to być np. dane teleadresowe osoby, jej numery dokumentów, dane finansowe, biometryczne, informacje o przynależności do organizacji, historia leczenia, dane geolokalizacyjne, lub np. informacje o jej poglądach w zakresie seksualności, polityki czy religijności. Regulacja dotyczy każdej osoby fizycznej. Osoby fizycznej się niektóre z głównych założeń RODO/GDPR, które powinny być respektowane:

 Dane osobowe obywateli powinny być przetwarzane zgodnie z prawem, uczciwie i w przejrzysty sposób.

 Osoby powinny zostać poinformowane, jakie dane i dla jakich celów są zbierane.

 Dane osobowe powinny być zbierane dla wyraźnie określonych i prawnie uzasadnionych celów. Nie mogą być wykorzystywane do żadnych innych działań, pozostających z nimi w konflikcie.

 Dane osobowe mogą być przechowywane i przetwarzane tak długo, jak wymaga tego zdefiniowany cel, ale nie dłużej.

 Przechowywane dane osobowe powinny być aktualne.



Osoby posiadają prawo do otrzymania kopii swoich danych. Mogą także wnioskować o zaprzestanie ich przetwarzania, a w niektórych wypadkach o całkowite ich usunięcie.



Organizacje powinny wdrożyć odpowiednie środki bezpieczeństwa w celu ochrony danych osobowych przed przypadkowym lub bezprawnym zniszczeniem, utratą, modyfikacją, czy ujawnieniem.



Personel organizacji, które przetwarzają dane osobowe powinien zostać odpowiednio przeszkolony w zakresie bezpieczeństwa i ochrony danych.

RODO/ GDPR wprowadza podejście oparte na ryzyku. Oznacza to, że środki ochronne stosowane przez organizację powinny być adekwatne do wrażliwości samych danych i ryzyka związanego z ich „wyciekiem”. Co za tym idzie: konieczna jest cykliczna analiza ryzyka, która pozwoli zweryfikować i zaktualizować środki bezpieczeństwa. W tym celu każda organizacja powinna zacząć od identyfikacji i udokumentowania procesów oraz związanych z nimi przepływów danych, a także wdrożyć procedury w zakresie prywatności i bezpieczeństwa. Istotne jest także prawne zobowiązanie organizacji do stosowania odpowiednich umów oraz weryfikowania należytej staranności w celu ochrony danych osobowych podczas przekazywania ich do podmiotów trzecich, w szczególności poza terytorium Unii Europejskiej. W przypadku „wycieku” danych osobowych, organizacja powinna zaraportować o tym w przeciągu 72 godzin od uświadomienia sobie incydentu. Nieprzestrzeganie przepisów wymaganych przez RODO/GDPR może skutkować grzywną sięgającą 4% rocznych obrotów przedsiębiorstwa, co czyni je jedną z najbardziej kosztownych finansowo regulacji na świecie.

Polski przekład

CERT Polska jest zespołem działającym w strukturach NASK powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w polskiej sieci Internet. Należy do organizacji FIRST, w ramach której współpracuje z podobnymi zespołami na całym świecie.

WWW: <http://www.cert.pl>

Redaktor Gościenny

Brian Honan jest dyrektorem generalnym BH Consulting z siedzibą w Dublinie, niezależnej organizacji zajmującej się cyberbezpieczeństwem i ochroną danych. Pracował jako doradca specjalny w Europol's Cybercrime Center (EC3), założyciel pierwszego irlandzkiego CERT'u. Członek rad konsultacyjnych w kilku innowacyjnych firmach z obszaru bezpieczeństwa. Znajdź Briana na LinkedInie: www.linkedin.com/in/brianhonan lub Twitterze [@brianhonan](https://twitter.com/brianhonan).



Przydatne linki

GDPR dla osób prywatnych i instytucji: <http://gdprandyou.ie>

Rozporządzenie GDPR: <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:32016R0679>

OUCH! Wydania archiwalne: <https://www.sans.org/u/D88>

Biuletyn OUCH! powstaje w ramach programu „Security Awareness” Instytutu SANS i jest wydawany na licencji [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/). Powielanie treści biuletynu jest dozwolone jedynie w celach niekomercyjnych oraz pod warunkiem zachowania informacji o źródle pochodzenia kopiowanych treści oraz nienaruszania zawartości samego biuletynu. Informacje kontaktowe: www.sans.org/security-awareness/ouch-newsletter. Editorial Board: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Polski przekład (NASK/CERT Polska): Sebastian Kondraszuk, Michał Strzelczyk, Jacek Sikorski