



Bezpieczeństwo danych - problemy i rozwiązania

Kompleksowe podejście do ochrony danych



Kompleksowa troska o cyberbezpieczeństwo to być albo nie być współczesnych firm. Mimo, że sukcesywnie rośnie świadomość znaczenia tego faktu, to przypadki naruszenia danych nadal dotyczą sporego odsetka przedsiębiorstw. W 2017 roku chociaż jeden taki incydent odnotowało aż 82% z tych działających w Polsce.¹

Informacje o tego typu przestępstwach regularnie goszczą w serwisach informacyjnych. W ciągu ostatnich kilku miesięcy wiele miejsca poświęcono również na dyskusję związaną z przepisami zawartymi w rozporządzeniu RODO.

Temat cyberbezpieczeństwa i konieczności sprostania nowym regulacjom związanym z ochroną danych osobowych dotyczy wszystkich na rynku niezależnie od wielkości czy branży. Warto przy tym podkreślić, że jedną z najważniejszych kwestii staje się kompleksowe podejście do tej sfery działania firmy.

¹ Raport "Barometr cyberbezpieczeństwa. Cyberatak zjawiskiem powszechnym", KPMG, styczeń 2018



Kontekst biznesowy

Musisz zadbać o prawidłowe przetwarzanie danych i zabezpieczenie informacji w Twojej firmie

Bez względu na charakter działalności, Twoja firma gromadzi i przetwarza informacje, które mają potencjalnie dużą wartość dla przestępców. Przechowujecie dużą liczbę danych osobowych i finansowych dotyczących pracowników. Natomiast dane kontaktowe klientów, które znajdują się w Waszych bazach mogą być wykorzystywane do popełniania oszustw lub wyłudzeń. Co więcej, jeśli Twoja firma świadczy usługi dla dużych korporacji, cyberprzestępcy mogą wykorzystać Cię jako furtkę do tych organizacji.

Podejście do kwestii ochrony danych osobowych zmieniło również wejście w życie nowych przepisów RODO. Każda firma, która przetwarza dane osobowe obywateli UE od 25 maja 2018 roku, ma obowiązek dostosować do nich swoje działania. Procesy związane z zarządzaniem i przetwarzaniem informacji muszą spełniać wysokie standardy bezpieczeństwa. Niezgodność będzie wiązała się z wysokimi karami finansowymi.

Jak więc zarządzać dokumentami w bezpieczny i uporządkowany sposób? Jak spełniając wszystkie wymagania dotyczące dostępności danych, jednocześnie zadbać o wysoki standard bezpieczeństwa? Co należy zrobić by zapewnić zgodność z przepisami zawartymi w RODO?

Zagrożenia



Zapewnienie bezpieczeństwa danych ma priorytetowe znaczenie. Wysoka kultura związana z zarządzaniem dokumentami przekłada się nie tylko na kwestie związane z ich ochroną ale również integralność i aktualność.

Brak zgodności z RODO może być bardzo kosztowny

Za brak zgodności z RODO firma może zostać ukarana grzywną w wysokości do 20 mln € lub 4% rocznych, globalnych obrotów.²

Utrata reputacji firmy

Brak dbałości o wysokie standardy związane z ochroną danych ma również bardzo poważne konsekwencje wizerunkowe, które mogą poważnie zagrozić pozycji rynkowej firmy.

Zgodność z przepisami i bezpieczeństwo informacji wymagają uporządkowania danych

Szacuje się, że 85% informacji biznesowych jest „nieuporządkowanych”. Oznacza to, że mogą znajdować się na urządzeniach osobistych pracowników lub w ich szufladach. Utrudnia to zrozumienie sposobu w jaki informacje przepływają w obrębie firmy³. Takie nieuporządkowane podejście do przechowywania informacji nie tylko zwiększa potencjalne ryzyko utraty danych, kradzieży lub ataku, ale utrudnia także rejestrowanie procesów i raportowanie zgodności z przepisami.

Wielkość firmy nie ma znaczenia

Cyberprzestępcy zagrażają wszystkim firmom bez wyjątku. Aż 60% małych i średnich firm (MŚP) przyznało, że doszło u nich do naruszenia bezpieczeństwa danych⁴. To samo dotyczy przestrzegania przepisów RODO.

² Portal UE EU GDPR, „Frequently Asked Questions about the incoming GDPR” na stronie www.eugdpr.org/gdpr-faqs.html

³ „A Guide to Improving Document Efficiency”, Biała księga Ricoh, październik 2013 r.

⁴ Badanie Quocirca Enterprise MPS, 2017 r. Zbiór danych: 240 organizacji zatrudniających ponad 500 pracowników z Wielkiej Brytanii, Francji, Niemiec i USA w różnych branżach.



Rozwiązania

Dostosuj firmę do wymagań RODO

Poleganie jedynie na dokumentacji w formie papierowej wiąże się z mniejszą dostępnością danych i rodzi większe ryzyko zgubienia czy zniszczenia ważnej umowy lub faktury. Wdrożenie elektronicznego obiegu dokumentów i elektronicznego archiwum pozwala na szybszy dostęp do ważnych danych, ułatwia kontrolę nad cyklem życia dokumentu i zapewnienie jego integralności. Przekonaj się, w jaki sposób firma Ricoh pomaga w digitalizacji, zarządzaniu i ochronie dokumentów.

Więcej funkcji zabezpieczających dane

Firma musi chronić dane w sposób kompleksowy i mieć na uwadze cały cykl życia dokumentu. Szczególnie, że obiegi dokumentów obejmują teraz znacznie więcej różnych urządzeń oraz sieci. Nie można pomijać żadnej z nich, a szczególnie środowiska druku. W ciągu ostatniej dekady zmieniły się możliwości i zadania, które wykonują nabiurkowe drukarki i wielofunkcyjne urządzenia drukujące. Odpowiadają za druk, cyfryzację i archiwizację dużej części dokumentów oraz danych firmowych. W związku z tym stanowią jedno z najistotniejszych, lecz często niedostrzeganych ogniw łańcucha obiegu danych. Wielofunkcyjne urządzenia drukujące Ricoh zapewniają dostęp do szeregu opcji podnoszących poziom bezpieczeństwa dokumentów m.in. szyfrowanie danych, PDF z cyfrowym podpisem, wydruk bezpieczny czy kontrola nieautoryzowanej kopii.

Pozbądź się danych, których nie potrzebujesz

Jednym z kluczowych wymagań RODO jest zapewnienie, że twoja firma przechowuje informacje tylko tak długo, jak są one potrzebne. W momencie, gdy dane są zbędne lub nie możesz mieć już do nich dostępu, musisz być pewien, że te zostaną skutecznie i bezpiecznie usunięte. Dotyczy to również informacji pozostawionych na urządzeniach wielofunkcyjnych po zakończeniu ich eksploatacji. Ricoh oferuje certyfikowaną usługę Data Cleansing, w jej ramach firma w bezpieczny sposób usuwa dane z urządzenia, po zakończeniu jego eksploatacji lub umowy.

Zgodność z przepisami RODO to szansa dla firmy

Regulacje związane z RODO mogą deprymować i wydawać się surowe. Stanowią jednak doskonałą okazję dla twojego biznesu do zweryfikowania obecnych procesów zarządzania informacjami. Wykorzystaj ten czas, aby precyzyjnie zidentyfikować i wyeliminować luki w obecnych zabezpieczeniach.



Ricoh Polska Sp. z o.o.
ul. Żwirki i Wigury 18A
02-092 Warszawa



(22) 256 15 55



www.ricoh.pl