# Czy jesteś gotowy na RODO?

GIODO
Generalny Inspektor Ochrony Danych Osobowych

## 7. Zabezpieczenia

Jednym z podstawowych celów ogólnego rozporządzenia o ochronie danych było dostosowanie zasad ochrony danych do wyzwań XXI wieku, takich jak internet rzeczy, czytniki RFID czy przetwarzanie danych w chmurze obliczeniowej. Prawo nigdy nie nadąży za rozwojem technologicznym, stąd też wiele przepisów rozporządzenia jest bardzo ogólnych i przede wszystkim technologicznie neutralnych (bez odniesień do konkretnych rozwiązań) – po to aby rozporządzenie zachowało aktualność także za 5 czy 10 lat. Efektem takiego myślenia jest przyjęta w rozporządzeniu koncepcja uwzględniania w każdym procesie przetwarzania danych ryzyka dla praw i wolności, jakie może nieść to przetwarzanie i każdorazowe dostosowywanie wykorzystywanych narzędzi zabezpieczających dane to tego ryzyka.

Każdy administrator danych zobowiązany jest do tego, by dane osobowe przetwarzał z poszanowaniem podstawowych zasad. W kontekście nadchodzących zmian szczególną uwagę warto zwrócić na zasadę integralności i poufności. Rozporządzenie definiuje ją tak: „Dane osobowe muszą być 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". Każdy, kto przetwarza dane osobowe, musi więc odpowiednio je zabezpieczyć, tak by uniemożliwić ich nieuprawnione udostępnienie.

W ogólnym rozporządzeniu nie znajdziemy jednak szczegółowych wskazówek, jakie środki organizacyjne i techniczne wdrożyć. Rozporządzenie zachęca jedynie do skorzystania z narzędzi pseudonimizacji czy też szyfrowania danych. W przepisach nie znajdziemy również minimalnych standardów technicznych bezpieczeństwa danych, a w maju przyszłego roku przestanie w dodatku obowiązywać rozporządzenie techniczne MSWiA do ustawy o ochronie danych osobowych (gdzie mamy chociażby wskazówki dotyczące częstotliwości zmiany hasła).

Zgodnie z zasadą rozliczalności, to administrator danych – uwzględniając aktualny stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres i cele przetwarzania danych – samodzielnie będzie decydował, jakie środki bezpieczeństwa wdrożyć, by zapewnić zgodność przetwarzania danych z wymogami rozporządzenia. Może więc uznać, że od maja 2018 r. nadal aktualne pozostaną środki techniczne i organizacyjne wdrożone i udokumentowane w dotychczasowej polityce bezpieczeństwa oraz instrukcji zarządzania systemem informatycznym, albo też podjąć decyzję o wdrożeniu zupełnie nowych środków.

Ważne, by oceniając stopień bezpieczeństwa przetwarzanych danych osobowych, uwzględnić przede wszystkim ryzyko wiążące się z przetwarzaniem – wynikające np. z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Ryzyko to może prowadzić do kradzieży tożsamości, straty majątkowej czy też naruszenia dóbr osobistych osoby, których te dane dotyczą. W sytuacji, kiedy doszłoby to takiego naruszenia ochrony danych, każdy administrator będzie zobowiązany do zgłoszenia tego faktu do GIODO, a w szczególnych przypadkach także do osób, których dane zostały naruszone.

W tym aspekcie pomocne może być stosowanie zatwierdzonych przez GIODO po 25 maja 2018 r. kodeksów postępowania. W tych właśnie dokumentach możliwe będzie doprecyzowanie przepisów ogólnego rozporządzenia, także tych dotyczących bezpieczeństwa danych. Grupa administratorów danych – np. zrzeszonych w izbie czy związku branżowym – może w opracowanym kodeksie zaproponować modelowe rozwiązania techniczne mające na celu zapewnienie poufności i integralności danych, a które będą ponadto bardzo pomocne dla wszystkich administratorów, którzy zobowiążą się do stosowania kodeksu.

Innym rozwiązaniem, dzięki któremu będzie można wykazać wywiązywanie się z obowiązku zabezpieczania danych, będzie stosowanie mechanizmu certyfikacji, czyli uzyskiwanie stosownych certyfikatów i znaków jakości potwierdzających właściwe zabezpieczenie danych osobowych.

Źródłem praktycznej i sprawdzonej wiedzy w zakresie budowy i zarządzania środkami bezpieczeństwa mogą być też, krajowe, europejskie lub międzynarodowe normy, w tym normy ISO.