Jak testować, mierzyć i oceniać skuteczność zabezpieczeń?

Posted on 2026-09-02

Wdrożenie odpowiednich środków bezpieczeństwa to jeden z podstawowych obowiązków administratora i podmiotu przetwarzającego. Nie jest to jednak czynność jednorazowa. RODO wymaga regularnego sprawdzania, czy zabezpieczenia rzeczywiście działają. Wyjaśniamy, co to oznacza w praktyce.

Obowiązek testowania

Zgodnie z art. 32 ust. 1 RODO administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych, a ich skuteczność podlega regularnemu testowaniu, mierzeniu i ocenianiu(lit. d). Przepis nie wskazuje ani metod, ani częstotliwości testowania – każdy podmiot dobiera je sam, stosownie do okoliczności przetwarzania.

Obowiązek ten ma charakter podstawowy i jest częścią szerszego, opartego na ryzyku podejścia do doboru środków. Systematyczna weryfikacja powinna obejmować cały system ochrony danych i dotyczyć zarówno skuteczności, jak i adekwatności zastosowanych

rozwiązań.

Zaniechanie nie niesie przy tym konsekwencji wyłącznie formalnych. Brak procedur zapewniających regularne testowanie może przyczynić się do wystąpienia naruszenia ochrony danych osobowych, a przy biernej postawie organizacji to właśnie incydent bywa pierwszym prawdziwym sprawdzianem skuteczności zabezpieczeń.

„Regularne”, czyli jakie?

Testowanie, mierzenie i ocenianie w sposób regularny oznacza świadome zaplanowanie i zorganizowanie takich działań, dokumentowanie ich oraz przeprowadzanie w określonych przedziałach czasowych, niezależnie od zmian w organizacji i przebiegu procesów przetwarzania[1].

Za niewystarczające należy więc uznać wyłącznie doraźne sprawdzanie skuteczności środków bezpieczeństwa, np. przy podejrzeniu podatności, przy zmianach organizacyjnych lub prawnych bądź w chwili wdrożenia. Zdarzenia szczególne powinny uruchamiać testy dodatkowo, a nie zastępować przyjętego harmonogramu.

Warto pamiętać, że choć przepisy nie określają wymaganej częstotliwości, odgórne przyjęcie cyklu rocznego nie daje automatycznej gwarancji. Jak przyjął Wojewódzki Sąd Administracyjny w Warszawie, przy takim upływie czasu skuteczność niektórych rozwiązań może w międzyczasie ulec dezaktualizacji[2]. Regularność testowania powinna być więc dostosowana do ryzyka i warunków konkretnego przetwarzania, a także do natury samych środków, z których każdy może wymagać innego cyklu oceny.

Nie tylko środki techniczne

W myśl art. 32 ust. 1 lit. d RODO regularnemu testowaniu, mierzeniu i ocenianiu podlega skuteczność środków nie tylko technicznych, lecz także organizacyjnych. Procedura działa bowiem wyłącznie wtedy, gdy jest stosowana, a szkolenie – gdy przekazywana na nim wiedza przekłada się na rzeczywisty poziom świadomości uczestników.

Przykładowo, o skuteczności regulaminu zakazującego korzystania z prywatnych nośników danych rozstrzyga to, czy zakaz jest faktycznie respektowany. W ocenie WSA w Warszawie szkolenie przeprowadzone rok przed naruszeniem ochrony danych osobowych może zaś okazać się niewystarczające[3]. Jego skuteczność wymaga zatem weryfikacji, zwłaszcza po pewnym czasie. To samo dotyczy procedury reagowania na incydenty – jej przyjęcie ma znaczenie tylko wtedy, gdy wskazane w niej osoby wiedzą, jakie czynności i w jakim czasie powinny wykonać w przypadku nieoczekiwanego zdarzenia.

Test musi być miarodajny

Nie każdy przeprowadzony test pozwala stwierdzić, że środki bezpieczeństwa rzeczywiście działają. Zdaniem WSA w Warszawie przegląd, który nie ujawnił istniejącej podatności, może świadczyć o nieskutecznym bądź niewłaściwym przeprowadzeniu i nie może zostać uznany za odpowiedni[4]. Nie oznacza to jednak, że testowanie musi być kosztowne. W przywołanej sprawie zabezpieczenie zostało wprawdzie zaprojektowane, lecz nikt nie sprawdził, czy przynosi zamierzony skutek. Jego weryfikacja nie wymagała ani specjalistycznej wiedzy, ani dużych nakładów finansowych.

Znaczenie ma też zakres testowania. Weryfikowanie zabezpieczeń wyłącznie pod kątem znanych podatności w oprogramowaniu, bez oceny ich adekwatności wobec

zidentyfikowanego ryzyka, wypełnia obowiązek jedynie częściowo[5].

Wskazówki co do samego „mierzenia” zawarte są w wytycznych EROD. Skuteczność można wyrazić wskaźnikiem ilościowym lub jakościowym, np. oceną ekspercką. Zamiast tego dopuszczalne jest także przedstawienie uzasadnienia oceny wybranych środków[6].

Testowanie a powierzenie

Wymóg testowania rozciąga się również na przetwarzanie powierzone. Jak wskazał Naczelny Sąd Administracyjny, korzystanie z usług podmiotu przetwarzającego nie zwalnia administratora z odpowiedzialności za bezpieczeństwo danych. Ciążą na nim dwa odrębne obowiązki: zapewnienie, aby taki podmiot wdrożył odpowiednie zabezpieczenia, oraz regularne testowanie ich skuteczności[7]. Jak z kolei stwierdził WSA w Warszawie, sama długotrwała współpraca, niepoparta okresowym i systematycznym przeprowadzaniem audytów lub inspekcji, nie gwarantuje, że powierzone zadania będą realizowane prawidłowo[8].

Ten sam kierunek wyznaczają wytyczne EROD, zgodnie z którymi operacje podmiotów przetwarzających powinny podlegać regularnym przeglądom i ocenom administratora[9]. Zakres i forma takiej weryfikacji powinny przy tym zależeć od charakteru współpracy i możliwości danej organizacji.

Co po teście?

Warto pamiętać, że test ma sens dopiero wtedy, gdy pociąga za sobą odpowiednią reakcję. To rzetelna analiza wniosków i realizacja zaleceń – nie sama ocena środków – podnosi ostatecznie poziom bezpieczeństwa danych.

W jednej ze spraw trzy kolejne audyty wskazywały na tę samą lukę w zabezpieczeniach. Mimo to została ona realnie usunięta dopiero po wystąpieniu naruszenia ochrony danych osobowych. W ocenie NSA wiedza o zagrożeniu połączona z brakiem realnych działań przesądziła o uznaniu naruszenia przepisów RODO za wynikające z niedbalstwa, co miało znaczenie przy wymiarze kary[10].

Testowanie a rozliczalność

Aby czynności weryfikacyjne spełniały wymogi RODO, powinny być także konsekwentnie dokumentowane. Obowiązek ten ma źródło w zasadzie rozliczalności, zgodnie z którą administrator musi być w stanie wykazać zgodność przetwarzania z przepisami (art. 5 ust. 2 RODO). Podmiot przetwarzający powinien zaś udostępniać administratorowi informacje niezbędne do wykazania spełnienia obowiązków wynikających z powierzenia (art. 28 ust. 3 lit. h RODO). W obu przypadkach samo zapewnienie o regularnym testowaniu, mierzeniu i ocenianiu skuteczności zabezpieczeń nie wystarczy. Konieczne jest udowodnienie, że czynności te rzeczywiście są wykonywane.

Przepisy nie określają formy takiej dokumentacji. W praktyce pomocne bywa odnotowanie daty i zakresu testu, zastosowanej metody, wykonawcy, poczynionych ustaleń oraz działań podjętych w ich następstwie. Pojedynczy zapis nie potwierdza jednak regularności, którą wykazać może dopiero ciąg takich zapisów lub harmonogram wraz z dowodami wykonania.

---

[1] Zob. wyrok WSA w Warszawie z dnia 21 czerwca 2023 r., II SA/Wa 150/23, utrzymany wyrokiem NSA z dnia 7 maja 2026 r., III OSK 2694/23.

[2] Zob. wyrok WSA w Warszawie z dnia 17 kwietnia 2024 r., II SA/Wa 1342/23 (nieprawomocny).

[3] Zob. wyrok II SA/Wa 1342/23, powołany w przyp. 2.

[4] Zob. wyrok WSA w Warszawie z dnia 21 października 2021 r., II SA/Wa 272/21; wyrok II SA/Wa 150/23, powołany w przyp. 1.

[5] Zob. wyrok WSA w Warszawie z dnia 16 września 2024 r., II SA/Wa 430/24 (nieprawomocny).

[6] Zob. EROD, *Wytyczne nr 4/2019 dotyczące artykułu 25. Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych*, wersja 2.0, przyjęte 20 października 2020 r., pkt 16.

[7] Zob. wyrok NSA z dnia 12 czerwca 2025 r., III OSK 1394/22.

[8] Zob. wyrok WSA w Warszawie z dnia 3 lipca 2025 r., II SA/Wa 2056/24 (nieprawomocny).

[9] Zob. EROD, *Wytyczne nr 4/2019…,* dz. cyt., pkt 39.

[10] Zob. wyrok NSA z dnia 26 czerwca 2025 r., III OSK 1312/24.