

W dobie narastających wycieków danych i coraz bardziej rygorystycznych regulacji dotyczących ich ochrony, bezpieczeństwo informacji przestało być wyłącznie domeną działów IT. Wiele firm inwestuje dziś ogromne środki w systemy informatyczne, audyty cyberbezpieczeństwa czy szkolenia pracowników. Tymczasem wciąż istnieje obszar, który bywa niedoceniany, a może prowadzić do równie dotkliwych konsekwencji: tradycyjna korespondencja papierowa.

Listy polecane zawierające wrażliwe informacje – rozliczenia, dane klientów, hasła, kody PIN, wyniki badań czy dokumenty finansowe – podlegają takim samym zasadom ochrony jak dane przetwarzane cyfrowo. RODO nie rozróżnia bowiem „danych z komputera” i „danych z koperty”. Każde ujawnienie informacji osobie nieuprawnionej może oznaczać naruszenie, a w konsekwencji również odpowiedzialność prawną i reputacyjną.

Skala naruszeń danych w systemach cyfrowych jest dobrze znana – według danych Urzędu Ochrony Danych Osobowych w 2023 roku administratorzy zgłosili ok. 7 tys. incydentów. Choć w przypadku korespondencji fizycznej problem występuje rzadziej, jego skutki mogą być równie poważne. Zdarzają się przesyłki zagubione, błędnie zaadresowane, dostarczone pod niewłaściwy adres lub odebrane przez osobę postronną. W przypadku dokumentów zawierających dane osobowe oznacza to ryzyko naruszenia ochrony danych – a więc sytuację, której firmy nie mogą już traktować jako „wpadki logistycznej”.

W tym kontekście coraz większego znaczenia nabierają technologie zabezpieczające dane w przesyłkach papierowych. W praktyce oznacza to, że ochrona informacji musi obejmować cały proces – od momentu przygotowania dokumentu aż po jego doręczenie.

W nowoczesnym podejściu do bezpieczeństwa korespondencji coraz częściej podkreśla się, że ryzyko ujawnienia danych nie dotyczy wyłącznie operatora pocztowego. Ochrona zaczyna się wcześniej: na etapie druku, personalizacji i konfekcjonowania przesyłek. Dlatego kluczowa staje się współpraca pomiędzy podmiotem odpowiedzialnym za produkcję korespondencji a tym, który ją doręcza.

Podkreśla się, że każdy papierowy dokument zawierający dane osobowe powinien być traktowany z pełnym reżimem bezpieczeństwa – dokładnie tak, jak system informatyczny przetwarzający dane klientów w bazach. W praktyce oznacza to konieczność wdrażania rozwiązań, które minimalizują ryzyko odczytania treści na każdym etapie obiegu.

Rynek usług pocztowych i poligraficznych coraz wyraźniej odpowiada na te potrzeby. W obiegu pojawiają się technologie, które sprawiają, że papierowa przesyłka staje się „bezpiecznym nośnikiem danych” – trudnym do podejrzenia, skopiowania czy przechwycenia bez pozostawienia śladów.

Jednym z rozwiązań są etykiety scratch code i code 09, stosowane do przekazywania kodów zastrzeżonych. Dane, takie jak PIN czy hasło, nanoszone są na etykietę i ukrywane pod warstwą ochronną – możliwe do odczytania dopiero po zdrapaniu lub rozciągnięciu zabezpieczenia. To prosty mechanizm, który znacząco ogranicza ryzyko nieuprawnionego wglądu.

Drugą popularną metodą są koperty PIN-owe i płacowe, czyli tzw. druki utajnione, które uniemożliwiają odczyt treści bez naruszenia dokumentu. Wykorzystuje się je zwłaszcza w branżach, gdzie korespondencja niemal zawsze zawiera dane wrażliwe, jak bankowość czy ubezpieczenia.

Coraz częściej stosuje się również druk typu pressure sealer – pojedynczy arkusz A4 lub składanki

## **RODO nie kończy się na komputerze. Papier też musi być bezpieczny**

Kategoria: Aktualności

Opublikowano: wtorek, 03, luty 2026 12:03

Tomasz Smaś

Odsłony: 521

---

perforowane z klejem aktywowanym naciskiem. Po zadrukowaniu i złożeniu na maszynie dokument sam staje się zaklejoną kopertą. To rozwiązanie nie tylko zwiększa bezpieczeństwo, ale też usprawnia proces masowej wysyłki.

Nowoczesna ochrona danych w korespondencji papierowej przestaje być dodatkiem, a staje się standardem w profesjonalnej obsłudze klienta. Coraz więcej firm wdraża rozwiązania kompleksowe – obejmujące cały proces „end-to-end”: od cyfrowego zlecenia, przez druk zabezpieczony i kopertowanie, aż po dystrybucję przez operatora pocztowego i doręczenie do adresata.

W czasach, gdy zaufanie klientów jest równie cenne jak sama usługa, zabezpieczenie korespondencji papierowej staje się nie tylko wymogiem prawnym, ale też elementem odpowiedzialności biznesowej. Bo w erze wycieków danych nawet zwykły list może być testem dojrzałości organizacji – i jej realnego podejścia do ochrony informacji.

*Źródło: IP*