RODO i komunikacja profesjonalna: dlaczego większość narusza przepisy nie wiedząc o tym

Prawie każde biuro, gabinet czy firma doradcza przesyła dokumenty z danymi klientów za pomocą aplikacji, których serwer znajduje się poza Europejskim Obszarem Gospodarczym. Bez złej woli, ale w wielu przypadkach naruszając rozporządzenie, o czym nikt ich nie ostrzegł.

Dokument, który podróżuje więcej niż myślisz

Codzienna sytuacja: doradca podatkowy otrzymuje komunikatorem dokument z danymi klienta. Handlowiec przesyła czatem ofertę do kolegi. Lekarka udostępnia tą samą drogą raport kliniczny koledze. Nikt nie myśli o tym dwa razy. To normalne. To wygodne. To właśnie robi się każdego dnia w każdym biurze w każdym mieście w Europie.

Ale ten dokument w wielu przypadkach właśnie odbył podróż na serwer w Stanach Zjednoczonych. Został zapisany – choćby tymczasowo, choćby "zaszyfrowany w spoczynku" – w chmurze, której ani profesjonalista, ani jego klient nie kontrolują. Przeszedł przez systemy, które technicznie mogą indeksować metadane powiązane z treścią. A europejskie Ogólne Rozporządzenie o Ochronie Danych ma w tej kwestii dość jasne zdanie.

Czego wymagają przepisy

RODO – i przez rozszerzenie orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej (w szczególności wyrok Schrems II, C-311/18, z 2020 r.) – stanowi, że dane osobowe obywateli europejskich muszą być odpowiednio chronione. Jeśli dane te opuszczają Europejski Obszar Gospodarczy, administrator danych musi zagwarantować, że odbiorca oferuje stopień ochrony "zasadniczo równoważny" europejskiemu. W praktyce oznacza to, że wysyłanie danych klientów za pośrednictwem usług, których serwery podlegają jurysdykcji USA, bez przeprowadzenia oceny skutków i wdrożenia dodatkowych zabezpieczeń – standardowych klauzul umownych, dodatkowych środków technicznych, takich jak weryfikowalne szyfrowanie itp. – może stanowić naruszenie rozporządzenia. Nawet jeśli nikt jeszcze nic nie powiedział.

I nie chodzi tylko o treść wiadomości. Metadane – kto co do kogo wysyła, kiedy, jak często, skąd – są również danymi osobowymi według przepisów, zgodnie z powtarzaną interpretacją Europejskiej Rady Ochrony Danych. Usługa zbierająca metadane z komunikacji zawodowej użytkownika przetwarza dane osobowe klientów tego użytkownika, bez ich wiedzy i bez udzielenia przez nich zgody na takie przetwarzanie.

Powszechny schemat myślowy – "używam aplikacji tylko do pisania; aplikacja nie jest dostawcą danych mojego klienta" – jest prawnie błędny. Jeśli dane klienta przechodzą przez infrastrukturę osoby trzeciej, ta osoba trzecia przetwarza te dane. A jeśli je przetwarza, musi istnieć podstawa prawna, umowa powierzenia przetwarzania i odpowiednie gwarancje.

Kto jest odpowiedzialny

Pytanie o to, kto ponosi odpowiedzialność prawną, nie jest akademickie. RODO rozróżnia *administratora danych* (kto decyduje o tym, jakie dane są przetwarzane i w jakim celu) i *podmiot przetwarzający* (kto robi to fizycznie, w imieniu administratora). Profesjonalista wysyłający dokumenty klientów jest administratorem. Dostawca aplikacji do przesyłania wiadomości jest w wielu przypadkach faktycznym podmiotem przetwarzającym. Bez umowy powierzenia – i bez większości klauzul, które taka umowa powinna zawierać – administrator nie dopełnił swojego obowiązku.

Łagodna interpretacja brzmi: "większość profesjonalistów o tym nie wie". Surowa interpretacja brzmi: "nieznajomość prawa nie zwalnia z jego przestrzegania". A interpretacja każdego prawnika specjalizującego się w ochronie danych, z którym się skonsultowano w tej sprawie, jest zazwyczaj surowa.

Dla kogo ma to znaczenie w praktyce

Dla każdego profesjonalisty lub firmy, która choćby okazjonalnie operuje danymi osobowymi osób trzecich:

- Prawnicy otrzymujący dokumentację od klientów (umowy, pozwy, zeznania, raporty majątkowe).
- Lekarze i inni pracownicy służby zdrowia udostępniający dane o zdrowiu – uważane za *szczególną kategorię* na mocy art. 9 RODO, z wzmocnionym reżimem ochrony –.
- Doradcy podatkowi i zarządcy administracyjni operujący danymi identyfikacyjnymi, podatkowymi i bankowymi.
- Działy zasobów ludzkich zarządzające dokumentacją pracowniczą i osobistą pracowników.
- Handlowcy otrzymujący dane kontaktowe i często wrażliwe informacje handlowe od potencjalnych i obecnych klientów.

W każdym przypadku informacje są chronione przez RODO. W każdym przypadku, w powszechnej praktyce, informacje te przechodzą kanałami, których jurysdykcja nie pozwala na uznanie ich za "zasadniczo równoważne" ramom europejskim bez dodatkowych zabezpieczeń. Nie ze złej woli. Z przyzwyczajenia. I przez infrastrukturę technologiczną, która przez piętnaście lat przedkładała wygodę nad zgodność.

Argument "wszyscy tak robią"

Warto przewidzieć najczęstszy zarzut: "jeśli wszyscy tak robią, to nie może to być realny problem". Jest to argument całkowicie zrozumiały i prawnie nie ma żadnej siły. Fakt, że praktyka jest powszechna, nie czyni jej zgodną z rozporządzeniem. Organy ochrony danych (np. polski UODO) nakładały w ostatnich latach kary na firmy właśnie za używanie komunikatorów, które wydawało się nieszkodliwe do momentu kontroli.

Obecna rzeczywistość operacyjna jest taka, że ryzyko jest niskie pod względem prawdopodobieństwa – bardzo rzadko zdarza się, aby kontrola organu nadzorczego audytowała konkretne narzędzia komunikacyjne średniej wielkości biura – ale wysokie pod względem skutków, jeśli się zmaterializuje. Jest to ryzyko, które większość podejmuje nie wiedząc, że je podejmuje. To znaczy, bez oceny, czy używane narzędzie jest zgodne z odpowiedzialnością prawną administratora danych.

Cyfrowy ślad jest wsteczny

Istnieje drugi argument, niemal symetryczny do poprzedniego, który warto przewidzieć: *"gdyby to był poważny problem, administracja już dawno zaczęłaby to kontrolować"*. Obecna zaobserwowana rzeczywistość przyznaje mu powierzchowną rację. Kontrole z powodu niewłaściwego korzystania z komunikatorów w małych firmach, a zwłaszcza u samozatrudnionych, są dziś niemal nieobecne – nie dlatego, że takie postępowanie jest dozwolone, ale dlatego, że administracji w większości krajów UE brakuje personelu niezbędnego do audytowania milionów zobowiązanych podmiotów.

To sugeruje dzisiejsza zaobserwowana praktyka. To nie jest to, co sugeruje następna dekada. Dwa wektory zbiegają się, aby zmienić tę równowagę w stosunkowo krótkim czasie.

Po pierwsze: cyfrowy ślad jest wsteczny. Każda wiadomość wysłana przez aplikację z serwerem centralnym zostaje zarejestrowana – przynajmniej w metadanych – w infrastrukturze, która trwa. To, co wysłano sześć miesięcy temu, jest technicznie nadal możliwe do skontrolowania dzisiaj. To, co zostanie wysłane dzisiaj, będzie możliwe do skontrolowania za pięć lat. Brak kontroli w teraźniejszości nie jest gwarancją braku kontroli w przyszłości. To odroczenie oceny, a nie zwolnienie z niej.

Po drugie: zdolność audytowa administracji będzie rosła w przyspieszonym tempie. Wprowadzenie narzędzi sztucznej inteligencji do procesów kontrolnych eliminuje ludzkie wąskie gardło, które do tej pory chroniło – faktycznie, nie prawnie – małe firmy i samozatrudnionych. System zdolny do krzyżowania masowych metadanych, deklaracji podatkowych, rejestrów handlowych i obowiązków powiadamiania o naruszeniach nie wymaga inspektorów: wymaga dostępu. A dostęp, poprzez wezwania do dostawców z obecnością prawną w UE, jest całkowicie wykonalny w obecnych ramach prawnych.

Do tego dochodzi czynnik mniej techniczny, ale równie decydujący: państwa europejskie znajdują się w procesie trwałego wzrostu zadłużenia i muszą, niemal bez wyjątku, poszerzać swoją bazę podatkową. Sankcja administracyjna wynikająca z nieprzestrzegania RODO jest, w kategoriach czysto fiskalnych, rosnącym i politycznie wygodnym źródłem dochodów. To nie przypuszczenie: to trend obserwowalny w rocznych sprawozdaniach europejskich organów ochrony danych, gdzie łączna suma kar rośnie od kilku lat z rzędu.

Wniosek operacyjny dla administratora danych nie jest alarmistyczny, ale chłodny: **decyzja o tym, jak zarządza się komunikacją z klientami dzisiaj, jest oceniana pod kątem zdolności kontrolnych roku, w którym nastąpi kontrola, a nie obecnych.** A te zdolności będą, w rozsądnym terminie, znacząco inne niż dzisiejsze. Kto zacznie robić rzeczy dobrze dzisiaj, będzie w porządku nie tylko od dzisiaj: ślad generowany od tego momentu będzie zgodny z przepisami, a to chroni wstecznie nadchodzący odcinek czasu. Kto będzie kontynuował dotychczasowe praktyki, będzie gromadził audytowalny ślad, którego zgodność będzie oceniana według standardów – i zasobów – nadchodzących lat.

Co zmienia się przy innej architekturze

Istnieją alternatywy techniczne, w których dane nie są przechowywane w infrastrukturze osób trzecich, lecz podróżują bezpośrednio z urządzenia nadawcy do urządzenia odbiorcy. W tej architekturze zgodność z RODO w zakresie przekazywania danych do państw trzecich nie zależy od standardowych klauzul umownych, ani od dobrej woli dostawcy, ani od przyszłych audytów. Zależy od tego, że *nie ma przekazywania*. A tego, co nie istnieje, nie można naruszyć.

To nie jest jedyne rozwiązanie ani jedyne możliwe. Ale jest strukturalnie inne, a zgodność z przepisami przestaje być proceduralnym dodatkiem, stając się bezpośrednią konsekwencją projektu. Dla profesjonalisty, który poważnie traktuje swoją odpowiedzialność jako administrator danych, ta różnica ma znaczenie.

Następne wydanie Cuadernos szczegółowo przeanalizuje wyrok Schrems II i jego praktyczne skutki dla małych i średnich firm zależnych od amerykańskich usług chmurowych, pięć lat po jego ogłoszeniu.

Źródła i ramy prawne

- Rozporządzenie UE 2016/679 (RODO), w szczególności rozdział V dotyczący przekazywania danych do państw trzecich.
- Wyrok TSUE w sprawie C-311/18 ("Schrems II"), 16 lipca 2020 r.
- EROD – Zalecenia 01/2020 w sprawie środków uzupełniających narzędzia przekazywania danych.
- UODO (i inne organy nadzorcze) – Raporty roczne z opisami kar za niewłaściwe korzystanie z komunikatorów w środowisku zawodowym.

← PoprzedniTajemnica zawodowa w erze cyfrowejNastępny →Gdy nie ma nikogo pośrodku

Ostatnie lektury

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Zabierz ten artykuł tam, gdzie go potrzebujesz.

↓ Markdown ↓ Zwykły tekst ↓ PDF

Plik zostanie pobrany na Twoje urządzenie. Stamtąd możesz go zapisać, zaimportować do Solo2 lub udostępnić w dowolnym miejscu. Cuadernos nie decyduje o miejscu docelowym za Ciebie.

Pieczęć lakowa · SHA-256 48324b78cc9dde51b2824d64c814a5e4b6cd08137d15aac2053b2a38ae0277d3

Cuadernos Lacre · Publikacja Menzuri Gestión S.L. ·
napisana przez R.Eugenio · redagowana przez zespół Solo2.